Teknik och samhälle
Datavetenskap och medieteknik

Examensarbete
15 högskolepoäng, grundnivå

En fallstudie inom en organisation av Security Operations Center (SOC): Utmaningar och utforskning av Agil och Traditionell metodik

A Case Study in a Security Operations Center (SOC) Organization: Challenges and exploration of Agile and Traditional Methodology

Sossio Giorgelli
Habib Mohammadi

Examen: Kandidatexamen 180 hp
Huvudområde: Datavetenskap
Program: Systemutvecklare

Handledare: Zahra Ghaffari Holmgren
Examinator: Patrik Berander
Datum för slutseminarium: 2024-08-26

Abstract

This study focuses on a specific organization of a Security Operations Center (SOC) as a case study to first identify specific challenges related to the work process, preceding with identifying which principles from various process models, such as agile and traditional methodologies from software development companies, can be implemented.

Initially, the study presents relevant research on agile and traditional process models as well as research on SOC. Subsequently, six semi-structured interviews are planned and conducted with employees within a specific SOC-type organization to identify the current work process and the challenges affecting the organization's work process.

The results of this study indicate a description of the current work process in the organization as well as a variety of challenges related to technical and organizational issues. Through analyses and discussions, the study deepened the challenges regarding the respondents' views, the current work process, and the connection to the described theories.

As a conclusion regarding RQ1, tools are the challenging aspects of technical challenges, while the organizational challenges are documentation, communication, and workload which have the greatest impact on the organization's work process. As a conclusion regarding RQ2, Scrumban's regular meetings and Kanban's board are the main principles that can be implemented in the organization's work process. For further research, the study suggests exploring how the implementation of Scrumban or Kanban can be carried out and conducting several case studies on multiple SOC-type organizations.

Keywords

Security Operations Center (SOC), Agile, Traditional

Sammanfattning

Studien inriktar sig mot en specifik organisation av Security Operations Center (SOC) som fallstudie för att i första hand identifiera specifika utmaningar kring arbetsprocessen och därefter identifiera vilka principer från olika processmodeller, så som agil och traditionell metodik från mjukvaruutvecklingsföretag, kan implementeras.

Inledningsvis presenterar studien relevant forskning kring agila och traditionella processmodeller samt forskning av SOC. Därefter planeras och genomförs sex semistrukturerade intervjuer med anställda inom en specifik organisation av SOC-typ för att identifiera nuvarande arbetsprocess och de utmaningar som påverkar inom organisationens arbetsprocess.

Resultatet av denna studie indikerar en beskrivning av den nuvarande arbetsprocessen i organisationen samt en variation av utmaningar kring tekniska samt organisatoriska utmaningar. Genom analyser och diskussioner ger studien ett fördjupad perspektiv på utmaningarna kring respondenternas syn, den nuvarande arbetsprocessen samt kopplingen till beskrivna teorier.

Som en slutsats kring FF1 är verktyg den utmanade aspekten från tekniska utmaningar medan organisatoriska utmaningar är dokumentation, kommunikation samt arbetsbelastning som är den största påverkan för organisationens arbetsprocess. Därmed blir slutsatsen att regelbundna möten från Scrumban samt Kanban board är den främsta principen som kan implementeras i organisationens arbetsprocess. För vidare forskning föreslår studien att utforska hur implementationen av Scrumban eller Kanban kan utföras samt utföra flera fallstudier kring flera organisationer av SOC-typ.

Nyckelord

Security Operations Center (SOC), Agil, Traditionell

Innehållsförteckning

1 Inledning

I en tid där cyberhot ständigt utvecklas och blir alltmer sofistikerade, spelar Security Operations Center (SOC) en avgörande roll i att skydda olika organisationers digitala tillgångar. SOC är en centraliserad säkerhetsenhet bestående av IT-säkerhetsexperter som kontinuerligt övervakar en organisations hela IT-infrastruktur [1]. SOC:s primära arbetsuppgift är att i realtid identifiera och hantera säkerhetsincidenter på ett snabbt och effektivt sätt, vilket säkerställer en proaktiv och stadig försvarshållning mot cyberhot [1]. Denna typ av SOC vägleder IT-organisationer genom identifiering och hantering av säkerhetsangrepp inom såväl mjukvaror som hårdvaror [2]. Numera utgör SOC en central komponent inom *små och medelstora företag* (SME) [1] vilket representerar en stor andel av alla företag inom EU samt kännetecknas av att inneha färre än 250 anställda [3]. Inom dessa sektorer av IT-organisationer tillämpas olika arbetsmetoder, även kallade *processmodeller*, vilka används för optimering av effektivitet i en verksamhet [4]. De olika arbetsmetoderna är *agil*, *traditionell*, en kombination av agil och traditionell samt kombinationer av olika agila arbetsmetoder [4], [5]. Inom agil processmodell arbetar arbetsgruppen iterativt [5] medan inom traditionell processmodell arbetar arbetsgruppen genom en linjär fas [6]. På grund av SOC:s betydande ansvar när det gäller att upprätthålla IT-säkerheten är det därför viktigt att utmaningarna inom en SOC:s processmodell är i minimal utsträckning samt att rätt arbetsmetod kan utnyttjas till en förbättring av incidentövervakning.

1.1 Tidigare forskning, Syfte och frågeställning

1.2.1 Tidigare forskning

Tidigare forskning har upplyst generella utmaningar inom SOC, samt specifika utmaningar relaterade till såväl mjukvara som hårdvara [7], [8]. Dessutom har tidigare forskning visat hur traditionella metoder hade kunnat ersättas med agila metoder inom specifika branscher som mjukvaruutvecklingsföretag [4]. Andra studier har även undersökt svårigheter med agila respektive traditionella metoder [9], [10] samt hur övergången från traditionell till agil metod har blivit genomförd med vägledning inom mjukvaruutvecklingsföretag [11], [12]. Ett forskningsgap uppkommer när tidigare forskning inom SOC behandlar allmänna utmaningar [7] utan att specifikt ta hänsyn till processmodeller. Dessutom har tidigare forskning belyst mindre kring SOC i relation med agil och traditionell processmodell.

1.2.2 Syfte

Med hänsyn till forskningsgapet, kommer därför denna studie inriktas mot en specifik organisation av SOC-typ för att i första hand identifiera specifika utmaningar kring arbetsprocessen och sedan vilka principer från olika processmodeller som agil och traditionell metodik från mjukvaruutvecklingsföretag kan implementeras.

1.2.3 Frågeställning

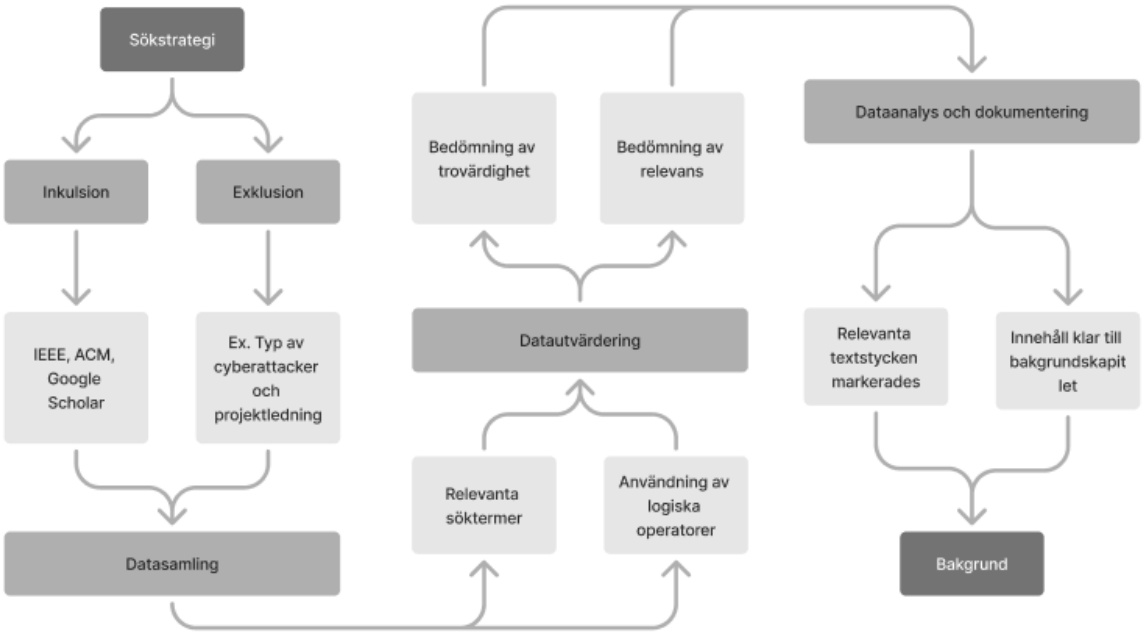
För att uppnå syftet kommer följande forskningsfrågor att besvaras:

- FF1: Vilka tekniska respektive organisatoriska utmaningar har ett framstående intryck på en specifik organisation av SOC-typ med den nuvarande processmodellen?

- FF2: Vilka principer från agil och traditionell processmodell från mjukvaruutvecklingsföretag kan implementeras på den nuvarande processmodellen för en specifik organisation av SOC-typ?

2 Sökstrategi

Detta avsnitt presenterar den sökstrategi som har använts i denna studie för att identifiera relevanta akademiska- och forskningspublikationer. Sökstrategin har i mycket stor utsträckning inspirerats från J. B. Oates [13]. Denna sökstrategi har varit väsentlig för sammanställningen av det teoretiska ramverket som presenteras under nästkommande avsnitt "3 Bakgrund". Som det nämndes i inledningen, har tidigare forskning belyst "SOC" samt "agil och traditionell processmodell" i mindre utsträckning. Med hänsyn till detta var det särskilt viktigt att tidigare forskning skulle framställs på ett noggrann sätt för att garantera tillräckligt med forskning för studiens bakgrund. Därför dokumenterades sökstrategin genom en beskrivning av utförandet. Utförandet av sökstrategi följdes enligt beskrivningen B. J. Oates [13, kap. 6] i fyra delar: Inklusion och exklusion, datainsamling, datautvärdering, dataanalys och dokumentering. Figuren nedan visar en överblick kring genomförandet av sökstrategier.



Figur 1: Överblick i sökstrategi.

2.1 Utförande av sökstrategi

2.1.1 Inklusion och exklusion

Inklusion och exklusion innebär att definiera kriterierna för vad som ska inkluderas samt vad som ska utelämnas [13]. Inklusionskriterierna innebär att inkludera relevant litteratur för specifika teman inom etablerade och trovärdiga databaser [13]. *IEEE* och *ACM* har valts som primära databaser med relevans för sökord som "agil", "traditionell" och "security operations center". Det har också varit relevant att inkludera liknande branscher som mjukvaruutvecklingsföretag som

tillämpar traditionell samt agil processmodell. Dessutom valdes *Google Scholar* med ingående databaser som *Emerald Insight*, *Springerlink* samt *Sage Journals* som sekundära databaser för att säkerställa en omfattande sökning av akademiska artiklar.

Till skillnad från inklusion, innebär exklusionskriterierna att utesluta irrelevanta litteratur som inte faller inom de angivna inklusionskriterierna [13]. Exempel på oväsentlig litteratur kan inkludera verk som inriktar sig på olika aspekter av cybersäkerhet snarare än hur SOC fungerar eller projektledningsstrategier snarare än beskrivning av agil arbetsmetod. Begränsningen bestod således i att fokusera på tidigare forskning baserat på arbetsmetoder inom både mjukvaruutvecklingsföretag och SOC, utmaningar kring SOC samt fall där agila eller traditionell processmodell är lämpliga för specifika sammanhang som incidentåtgärd.

2.1.2 Datainsamling

Efter att Inklusion och exklusion identifierades, formulerades söktermer för datainsamlingen som presenteras i form av bilagor, *Bilaga 1: Redovisning av sökföranden*. Bilaga 1 presenterar tabeller med databaser, sökord och sökresultat. De gråmarkerade rutorna i tabellen anger att en eller flera artiklar har hittats från ett specifikt sökord. Varje tabell visar samtliga sökord inom de tre databaserna IEEE, ACM och Google Scholar. Dessutom tillämpades avancerad sökfunktion för att undvika förväxlingar med förkortningar och för att säkerställa att de erhållna sökträffarna var relevanta [13]. För specifika sökfraser användes logiska operatorer, främst "AND" för att specialisera relevansen och "OR" för att hitta ytterligare akademisk litteratur. Sökorden som visas i bilaga 1 framställer att sökord med citattecken och/eller operationen “AND” gav färre och mer specifika resultat i jämförelse med dem utan citat och/eller operationen med “OR”. Även om sökresultatet framställde stort antal resultat, var många orelevanta för denna studien då de var inriktade mot ämnet som cybersäkerhet för sig själv eller agil för sig själv. Samtidigt, användningen av långa sökord utan citattecken eller långa sökord med “OR” gav omfattande resultat. Prioriteringen av sökorden var således att vara mer specifik med användning av citattecken och operationen “AND”. Upphittade artiklar, det vill säga artiklar som var relevanta för uppsatsens bakgrund, visas i andra kolumnen i de tre tabellerna i bilaga 1.

Dessa sökord är de väsentliga sökorden som tillämpats under sökprocessen: "agile", "traditional", “waterfall”, "small medium enterprise" och "security operations center". Dessa söktermer har fördjupats för att säkerställa att tillräckligt relevant forskningsmaterial till bakgrundskapitlet finns med, vilket presenteras i bilagor, *Bilaga 2: Omfattning av material*. Tabellen i bilaga 2 visar sökningar med relevanta sökord till denna studie. Sökningarna gjordes i “All metadata” och utfördes först den 21 februari 2024. Ytterligare sökningar har utförts i efterhand för att vara uppdaterade med ny vetenskaplig forskning nära ämnet. Tabellen är även associerad med samtliga venndiagram som visas nedanför tabellen i bilaga 2 för att överblicka sökresultatet ytterligare. Enligt

tabeller och beskrivningar i de föregående bilagorna, visas det tydligt relevanta artiklar. För att säkerställa att samtliga relevanta artiklar identifierades, genomfördes en ytterligare prioritering av omfattande sökord inom de tre angivna databaserna. Den första tabellen i bilaga 2 samt underliggande venn-diagram visar enskilda söktermer inom konceptet A: agil och traditionell, A2: utökad variant av A, B: small medium enterprise och C: security operations center. För specifika sökningar utfördes kombinationen av söktermerna enligt den andra tabellen, vilket gav mindre resultat. Det är bra att notera att de sista två raderna i den andra tabellen ("A & B & C" och "A2 & B & C") gav den slutliga omfattningen som skulle vara relevant för att öka garantin att all relevant akademisk forskning har upphittats.

2.1.3 Datautvärdering

Efter datainsamlingen genomfördes en noggrann datautvärdering, vilket innebär att vetenskapliga artiklar söktes fram och granskades noggrant för att bedöma deras trovärdighet och relevans. Trovärdigheten kring Google Scholar bedömdes med hänsyn till författarens bakgrund, publiceringsår, antal citeringar samt vilka andra forskningsartiklar som de refererade till. Granskningen baserades främst på abstrakten för att bedöma artiklarnas relevans för studiens syfte. Därefter granskades innehållet i de utvalda artiklarna för att säkerställa att de var relevanta för studien. De upphittade artiklarna som har granskats, numrerades för att underlätta identifieringen och åtkomsten. En omfattande litteraturgenomgång genomfördes för att kartlägga tidigare forskning. Baserat på detta visas en matris som presenterar olika koncept som presenteras i bilagor, *Bilaga 3: Kategorier av artiklar*.

2.1.4 Dataanalys och dokumentering

Efter att ha genomfört datainsamling och utvärdering gjordes en noggrann dataanalys. Genom att läsa de vetenskapliga artiklarna markerades relevanta meningar och stycken. Därefter genomfördes en analys av de markerade delarna för att extrahera viktig information relaterad till studiens teoretiska bakgrund, syfte och frågeställningar. Genom denna process identifierades och sammanställdes viktiga teman, trender och mönster som framkommit i litteraturen. Baserat på de betydelsefulla markeringarna och den genomförda analysen dokumenterades för bakgrundsavsnittet. Bakgrund presenterades på ett strukturerat och översiktligt sätt vilket möjliggjorde en klar och transparent redovisning av den erhållna forskning.

3 Bakgrund

Detta avsnitt presenterar tidigare forskning kring agil, traditionell, SOC och relevanta teorier kring studiens ämne. Det finns ett omfattande antal studier om processmodeller, särskilt om agil och traditionell metodiken inom IT och mjukvaruutvecklingsföretag. Studierna [4], [14], [12], [6] visar potentiella användningsområden av agila och traditionella metoder inom olika mjukvaruutvecklingsföretag. Dessutom finns det forskning som belyser hur SOC arbetar samt de utmaningar som är aktuella [1], [7], [8].

3.1 Agil och traditionell processmodeller

3.1.1 Historisk översikt

Drygt från slutet av 1980-talet till början av 1990-talet har det bästa möjliga sättet att utveckla mjukvara blivit behandlad med noggrannhet, detaljerad projektplanering, dokumentation och systemarkitektur [15]. Denna arbetsmetod för mjukvaruutveckling benämns som traditionell metodik, även känd som planstyrd metodik. Inom en mjukvaruutveckling omfattar alla aspekter av mjukvaruproduktion från den initiala idén till drift och underhåll [16]. Faserna för denna mjukvaruutveckling omfattar kravspecifikation, design och implementation, test, drift och underhåll [16]. Samtidigt har större grupper ofta varit involverade i omfattande projekt för leverans av mjukvara inom ramen för dessa traditionella metoder [15]. Inom den traditionella metoden har begränsningarna såsom tydliga kravställningar medfört att det har blivit frustration med att använda en sådan väldefinierad och tung arbetsmetod. Under 1990-talet introducerades en alternativ arbetsmetod, den agila arbetsmetoden, som inriktade sig mer på själva mjukvaran än på design och dokumentation [15]. Den agila arbetsmetoder kan också betraktas som en itererad variant av traditionell metod med fokus på mjukvaran [15]. I början av år 2001 introducerades sedan det agila manifestet med fyra principer som tog mjukvaruutveckling till en annan nivå. De fyra principerna lyder följande:

- *"Individuals and interactions over processes and tools.*
- *Working software over comprehensive documentation.*
- *Customer collaboration over contract negotiation.*
- *Responding to change over following a plan."* [15], [17].

Detta indikerar att agila manifestet lägger stor vikt för individen, fungerande mjukvara, samarbete samt anpassningsbarhet. Utifrån dessa fyra principer har agila arbetsmetoder utvecklats, vilket för sex år sedan används mest inom många företag [15].

3.1.2 Agil processmodell

Agil är en processmodell som syftar till att hantera föränderliga krav där kunden är involverad i utvecklingsfasen [5]. De agila arbetsmetoderna är anpassningsbara [6], vilket innebär att ändringar, lägre kostnader, minskning av tidsramar samt kvalitetsproduktioner kan utföras på ett tillfredsställande sätt [14]. Agila arbetsmetoder är dessutom lättviktiga processmodeller som främjar interaktioner mellan intressenter för att snabbt producera mjukvara av hög kvalitet [5]. Inom agila arbetsmetoder ingår metoder såsom Extreme Programming (XP), Scrum, Crystal med flera [4]. Dessa metoder har blivit adopterade inom olika områden av mjukvaruutveckling med fokus på individuella interaktioner, processer, verktyg, dokumentation, nära relation med kunden och responsivitet mot ändringar i plan [4]. Genom en kombination av dessa agila arbetsmetoder blir det till en så kallad agil-hybrid arbetsmetod [4]. I modern mjukvaruutveckling har användningen av agila metoder blivit allt vanligare nuförtiden. För att förstå deras olika tillämpningar och fördelar är det av yttersta vikt att noggrant granska dem.

Enligt B. Bruiners et al. [4] är de kända agila metoder Extreme Programming (XP), SCRUM, Dynamic Software Development Method (DSDM), Adaptive Software Development, Crystal, Feature-Driven Development (FDD), Lean Development och Hybrid Agile Method (Scrumban). För varje metod specificeras även hur verktygen kan bedömas bli effektiva:

- **Extreme Programming (XP):** Denna metod är en snabb och iterativ utveckling som utförs för mindre grupper. Kvalitetsprodukter rankas mycket högt tillsammans med en snabb leverans [4]. Verktyget ligger till relation med snabb leverans och hög kvalitet [4].

- ***SCRUM*:** Denna metod är ett ramverk för att hantera komplexa projekt. Det organiserar arbete i korta, iterativa sprintar och främjar samarbete och kommunikation inom gruppen [4]. Verktyget kan anses bli relaterat till korta sprintar samt tät samarbete inom gruppen och frekventa möten [4].

- **Dynamic Systems Development Model (DSDM):** DSDM är en metodik som är kundcentrerad och iterativ. Den betonar att vara flexibel nog, att svara på förändrade krav och att involvera kunden under hela utvecklingsprocessen [4]. Verktyget ligger till att främja flexibilitet av förändring [4].

- **Adaptive Software Development (ASD):** ASD är en metod som fokuserar på att hantera osäkerhet och förändring genom att vara adaptiv och flexibel i en stor grupp. Denna arbetsmetoden betonar att kontinuerligt anpassa sig till förändrade förutsättningar och att lära av erfarenheterna [4]. Verktyget anses att främja flexibilitet av förändring [4].

- **Crystal:** Crystal är en serie av metoder som varierar beroende på projektets storlek och komplexitet. Den riktar sig på att anpassa utvecklingsmetoder efter specifika projektbehov och främjar samarbete och kommunikation inom gruppen [4]. Verktyget anses vara anpassat efter storlek av projekt [4].

- **Feature-Driven Development (FDD):** Metoden inriktar sig på utformning av den övergripande produkten. Efter klar produkt sammanställs en funktionslista av den faktiska produkten [4]. Verktyg anses vara relaterade till dokumentation av funktionslista [4].

- **Lean Development:** Metoden fokuserar på att minimera slöseri och maximera effektiviteten genom att leverera lösningar så snabbt som möjligt. Detta uppnås genom att eliminera onödiga steg och processer [4]. Eftersom metoden utförs snabbt, faller kvaliteten av produkten. Det initiala verktyget som kan tolkas är de processer som utförs hastigt [4].

- **Hybrid Agile Method (Scrumban):** En metod som kombinerar Scrum och Kanban. Scrumban ger flexibiliteten hos Kanban och strukturen hos Scrum. Detta tillåter en grupp att anpassa sig till förändrade krav och prioriteringar på ett snabbt sätt genom att hålla regelbundna möten [4]. Verktyget ligger kring kombinationen av scrum och kanban.

Som en annan agil arbetsmetod, ingår även Kanban:

- **Kanban:** Kanban är en processoptimering för att organisera kunskap om olika aktiviteter bland olika deltagare på ett visuellt sätt [9]. I Kanban systemet förekommer det så kallade kort som innehåller förklaring om arbetsuppgift som tilldelas inom en grupp vilket senare utförs och sedan förflyttas korten mot mål baserat på olika status som till exempel ej börjat, pågående och klar [18]. Verktyget belyser kring tavla med status av arbetsprocessen [18].

Sammanfattningsvis, är agila arbetsmetoder flexibla processmodeller som hanterar föränderliga krav med kundens involvering. De främjar snabb produktion av högkvalitativ mjukvara genom interaktioner mellan intressenter [4], [5], [6], [14].

3.1.3 Traditionell processmodell

Till skillnad från agila arbetsmetoder, är däremot traditionell en linjär fas i utveckling [6]. Traditionell arbetsmetod är oftast följdriktiga med brist på anpassningsbarhet och har oftast lägre förmåga att kunna göra ändringar i tidigare faser [19]. Trots att de flesta företag använder agila arbetsmetoder nuförtiden [20] är traditionella metoder fortfarande relevanta [5]. Detta kan bero på att organisationer med traditionell processmodell tar en noggrann hänsyn till produkter som kan relatera till säkerhetsaspekter [20]. Inom traditionell arbetsmetod ingår olika metoder som också kan kallas för *tungvikta metoder* [21]. Dessa metoder är Vattenfallsmodellen, Unified Process (UP) och Spiralmodellen:

- **Vattenfallsmetoden:** Denna metod är den kända metoden som oftast har 6 faser som analys, design, utveckling, testning, implementation och underhåll [5]. Av namnet betonas att processer utförs som en rinnande "vattenfall" [21].

- **Unified Process (UP):** Denna metod utförs på ett iterativt och inkrementellt sätt. Iterationen utförs med 4 faser: inledning som bland annat definierar genomförbarhet, utarbetning där arkitektur tas fram, konstruktion där produkten byggs upp och övergång där produkten introduceras till intressenter [21].

- **Spiralmodellen:** Precis som UP, utförs denna metod också ett iterativt och inkrementellt sätt. Denna metod skiljer från UP då prototyping av produkten utförs som en del av varje inkrement [21].

Inom samtliga traditionella arbetsmetoder tillämpas dokumentationsrelaterade verktyg som är en avgörande del i en traditionell metod [21]. Inom dokumentation dokumenteras exempelvis arkitektur av system med verktyg som Unified Model Language (UML) [21]. Med det sagt, traditionella arbetsmetoder är linjära och mindre anpassningsbara, vilket gör det svårt att ändra tidigare faser [19]. Trots att agila metoder är vanligare idag, är traditionella metoder fortfarande relevanta, särskilt för produkter med säkerhetsaspekter [20], [5].

3.1.4 För- och nackdelar med agil och traditionell

Emellertid har agil dock sina egna fördelar och begränsningar [4]. Fördelar och nackdelar visas med användning av agila metoder i olika delar av arbetet. A. Mishra et al. [9] har studerat viktiga områden om agila metoder i olika situationer av agila utvecklingsprocess via enkätundersökning där studien har visat att observationer har gett resultat som visar många fördelar med agila utvecklingsprocess. Dessa fördelar inkluderade bättre kommunikation och koordination, utvecklad kvalitet, bättre produktivitet och högre moral. Samtidigt finns det en studie av R. Mokhtar [19] som visar att det finns potentiella nackdelar såsom brist på experter och resurser i agila

utvecklingsprocess. R. Bin-Hezam et al. [15] nämner sedan att SME brukar arbeta med små projekt och uppgifter jämfört med stora organisationer och därför är agila metoder bäst passande inom dessa situationer. Med detta betonas det att små ändringar under processen kan ske med agil process medan det traditionella arbetssättet inte ger rum till att återvända eller göra konstant ändring i mitten av processen. Däremot, är traditionella metoder som vattenfallsmodell lämpliga för projekt med väldefinierade krav med en utmärkt uppfattning av tekniska verktyg [22]. Å andra sidan, är nackdelarna med vattenfallsmodellen är att de är ofta strikta, ställer hårda krav och tappar relevansen gradvis [23]. Till skillnad från traditionell, har agila dessutom bedömts att vara effektivare än traditionell [23], där effektivitet definieras som en mätning av hur bra en IT organisation utvecklar rätt tekniska komponenter i affärslösningar för sina kunder [24]. Enligt [22] finns det också egenskaper som skiljer mellan traditionell och agil:

- Kraven är högre i traditionell än i agil.
- Klient involvering inom traditionell är lägre medan i agil är det större.
- Omfattningen av projekt är större i traditionell än agil.
- Organisationen inom traditionell är hög formalisering medan agil är flexibel.
- Dokumentationen är formell i traditionell än i agil.

Med det sagt har agil och traditionell arbetsmetod både fördelar och nackdelar. Fördelarna inom agil inkluderar bättre kommunikation, kvalitet, produktivitet och moral, medan nackdelarna kan vara brist på experter och resurser [15]. Agila metoder passar särskilt bra för SME med föränderliga krav, till skillnad från traditionella metoder som vattenfallsmodellen, som är bättre för projekt med väldefinierade krav. Dock är processen för vattenfallsmodellen oftast striktare än processen för agil [23].

3.1.5 Empiriska studier kring hybrid processmodell

En kombination av traditionella och agil processmodeller utgör en hybrid processmodell [5]. Detta innebär att vissa delar av arbetsprocessen är agil medan andra delar följer en traditionell metodik, oftast vattenfallsmodell [5]. En studie av N. Yahya et al. [5] resonerade val av hybrid metod genom intervjuer som kom fram till en kombination av Scrum och traditionell. Anledningen bakom kombinationen av Scrum och traditionell har betonats av projektets komplexitet. Dessutom har N. Yahya et al. nämnt att den typ av metod har använts mest för att utveckla mjukvara. Det hävdades att traditionellt ensamt inte är tillräckligt för att uppfylla en viss organisationens behov [5]. Studien påpekade också att ingen ensam metod kunde bli applicerad universellt till alla projekt [5]. Därför har det betonats närvaro av hybrid metoder som en nyckelaspekt till organisationer. En annan studie av W. Singhto et al. [22] har studerat också att blanda traditionella och agila metoder för ett litet projekt av programvaruutveckling, särskilt för SME. Studien enligt W. Singhto et al. har tagit slutsatser att blandningsmetoder kan förbättra projektresultat men måste anpassas för specifika behov av projekt. Inom dessa två situationer har forskningen visat att en hybrid av agil och traditionell utökar möjligheterna av projektarbetet.

En annan studie av A. Mishra et al. [9] har däremot utfört undersökning genom att skicka frågeformulär till 52 mjukvaruföretag i 7 olika länder. Dessa har analyserats kvantitativ om huruvida agila metoder är bra för SME och dess faktorer som påverkar projektet. Undersökningen gjordes inte bara inom SME utan även i andra storlekar av företag och i olika länder. Statistiska resultat visade att de flesta företag föredrar att använda agila metoder i kombination med andra arbetsmetoder. På liknande sätt har en annan undersökning enligt E. C. Conforto et al. [10] bevisat genom frågeformulär där 19 företag inom SME med traditionella arbetsmetoder kämpar för användning av sina nuvarande förvaltningspraxis inför olika projektutmaningar. Vidare nämns det att utveckla hybrid liknande metoder för olika industrier. Dessa undersökningar visar en väg till en kombination av både agil och traditionell metod. Enligt en ytterligare undersökning med 247 deltagare från 23 länder av M. Kassab et al. [20] visade studien att många av mjukvaruutvecklingsföretag använder agilt mer än traditionellt medan IT säkerhetsföretag använder hälften agilt och hälften traditionellt. Med det sagt använder de flesta IT säkerhetsföretag jämt fördelat mellan agil och traditionell metod. Vidare har A. Mishra et al. [9] och E. C. Conforto et al. [10] undersökt användning av agila metoder inom SME och identifierade faktorer som påverkar deras implementering och produktivitet. Detta resonemang utvidgas av M. Kassab et al. [20], som tar upp frågan om att blanda traditionella och agila metoder och dess effekt på organisationers arbetsprocesser.

3.3 Security Operations Center

3.3.1 Generell beskrivning av SOC

Som tidigare omtalades, övervakar SOC hela IT-infrastrukturen dygnet runt för att upptäcka och hantera larm i realtid på ett snabbt och effektivt sätt [1]. Ett SOC fungerar som en grupp av skickliga människor som arbetar med definierade processer och stöds av integrerade tekniker med säkerhetsunderrättelse [25]. SOC kan antingen implementeras internt av ett företag eller köpas som en tjänst från andra leverantörer av säkerhetstjänster [2]. Huvudfunktionerna för en SOC är att övervaka händelser som berör säkerhet och cyberhot från distribuerad säkerhet samt ge svar på dessa händelser. Genom dessa huvudfunktioner kan SOC ha situationsmedvetenhet, minska risker samt hjälpa till med att förebygga olika hot [2]. SOC fokuserar specifikt på cyberhot, övervakning, kriminalteknisk utredning och incidenthantering och rapportering [25]. En SOC kan också tilldelas andra uppgifter såsom hantering av säkerhetskontroller, övervakning av tillgänglighet och tillgångar [2]. Med det sagt, utför SOC kontinuerlig övervakning, men även insamling av loggdata [25]. Alla samtliga aktiviteter samt möjligheter med SOC kan anges med tre kategorier [1]:

- **Förberedelse, planering och förebyggande:** Här hanterar SOC lager av tillgång som exempelvis applikationer, databaser, servrar och molntjänster. Rutinunderhåll och förberedelser utförs också genom att uppdatera säkerhetspolicyn. SOC utför också planering av incidentrespons, regelbundna tester och hålla sig uppdaterad om de senaste säkerhetslösningar [1].

- **Övervakning, upptäckt och respons:** Här övervakar SOC hela IT infrastruktur på 24/7/365, hanterar loggar som innehåller analysdata om säkerhet, hantering av hot från obehörig användare, automation med moderna verktyget SIEM (Security information and event management) samt respons av hot [1].

- **Återställning, förfining och efterlevnad:** Här utför SOC återställning för exempelvis lösenord, utför förfining genom att uppdatera processer, policys och alternativa verktyg för cybersäkerhet. SOC är även ansvarig för hantering av efterlevnad som berör applikationer, system och säkerhetsverktyg samt processer att de följer bestämmelser av datasekretess såsom GDPR [1].

En SOC utgör också fördelar såsom snabba svarsfunktioner för skydd av tillgång, implementation av effektiva säkerhetsåtgärder, kostnadsbesparingar, kundförtroende samt förbättrad incident respons [1].

Inom SOC finns det även olika roller som har olika ansvarsområden [1]:

- **SOC chef:** Driver medarbetarna och övervakar alla säkerhetsoperationer.
- **Ingenjör inom säkerhet:** Bygger ut samt hanterar organisationens säkerhetsarkitektur.
- **Analytiker inom säkerhet:** Hanterar de första larm som cyberhot eller incidenter som dyker upp.
- **Andra specialister:** Det finns andra specialister beroende på organisationens storlek.

3.3.2 Utmaningar inom SOC

Inom forskningen kring SOC har det identifierats flera utmaningar relaterade till arbetsprocesserna. En systematisk litteraturstudie har utförts av M. Vielberth et al. [7] som har belyst en brist på akademiska artiklar som fördjupar förståelsen av SOC, särskilt när det gäller beskrivning av arbetsmetoder. En av de centrala utmaningarna är bristen på automatisering inom SOC, vilket leder till en betydande manuell arbetsbelastning. Detta ökar risken för fel och kan försena svarstiden vid hantering av säkerhetsincidenter. Vidare identifierar F. D. János et al. [8] olika bekymmer av säkerhet inom SOC som främst är relaterade till teknik, såsom mjukvaru- och hårdvaruproblem. Dessa bekymmer kan inkludera svårigheter med att integrera och underhålla olika säkerhetsverktyg och plattformar, vilket kan skapa komplexitet och sårbarheter i SOC. Dessa tekniska utmaningar påverkar direkt arbetsprocesserna inom SOC och kan hindra effektiv incidenthantering och svar på hot. En annan viktig aspekt är klassificeringen av SOC. Studien av P. Jacobs et al. [2] framhäver en brist på tillräckliga referenser i industri ramverk för att klassificera SOC. Detta kan leda till otydlighet i SOC och ansvarsområdena, vilket i sin tur kan påverka effektiviteten i arbetsprocesserna. En tydlig och enhetlig klassificeringsmodell är avgörande för att säkerställa att arbetsuppgifter och ansvarsområden är tydligt definierade och förstådda inom SOC [2].

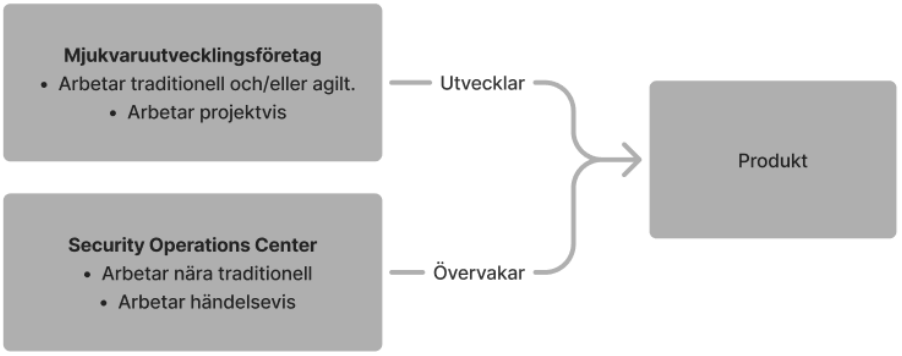
Inom SOC följer det särskilda riktlinjer och används verktyg i form av mjukvaruverktyg som program [1]. Trots användningen av verktyg för att visa larm kvarstår en betydande arbetsbelastning, eftersom många larm kan inträffa samtidigt och det tar längre tid att åtgärda dem, enligt analyser av M. Vielberth et al. [7]. Verktyg i form av automatisk detektion av hot kan på ett bra sätt hantera välbekanta attacker [7]. Dessa verktyg måste också bli underhållna vilket kräver mycket resurser och tid [7]. En utmaning med verktyg inom SOC är att de ofta väljs baserat på budgetrestriktioner snarare än deras faktiska användbarhet och effektivitet [7]. Kring riktlinjer och policyer anges det att missbruk av policy kan med hjälp av rutinmässig analys identifieras samt minskas enligt en studie av A. Madani et al. [26]. Dessutom pekar studien av A. Madani et al. [26]

på utmaningar relaterade till logghantering inom SOC. Denna logghantering kan även tolkas som dokumentation där personal dokumenterar åtgärder det gör för varje larm. Logghantering är en kritisk del av SOC:s verksamhet för att spåra och analysera säkerhetshändelser [26]. Bristande logghantering kan leda till förlust av viktig information, vilket i sin tur kan försvåra incidenthantering och respons [26].

Inom SOC är samarbete och kommunikation kring olika personal väsentliga för att det ska vara så effektivt som möjligt [7]. Inom samarbete är det kompetensutveckling som bör vara aktuell för en bra förståelse och kommunikation [7]. I samband med det kan kompetensutveckling för nya personal utföras genom konferenser för att utbilda personal till en högre utbildningsnivå [7]. Detta är mycket fördelaktigt för att öka anställdas professionalitet. Däremot är kompetensutveckling en svårighet som ökar med tiden [7]. Som en del av kompetensutveckling, rör det aspekter om planering och möten. Planering ingår vanligtvis inte för SOC som en process då de hanterar larm baserat på hur mycket larm det tillkommer [2]. Dock förekommer möten i SOC där personal ställer upp frågor och tillför förbättringar inom samarbetet [7]. Det är värt att notera att tidigare forskning inte har belyst utmaningar som uppstår vid planering och möten i relation till SOC. Detta öppnar upp för framtida studier att utforska dessa viktiga aspekter och bidra till en djupare förståelse av SOC:s operativa effektivitet.

3.3.3 Processmodeller inom SOC

Som det har nämnts innan, har tidigare forskning kring SOC och arbetsmetoder som agil eller traditionell arbetsmetod belysts mindre inom ramen av forskning. Detta gav en möjlighet att utforska SOC med processmodeller genom forskning som är relaterat till mjukvaruutvecklingföretag. Faktum är att både SOC och mjukvaruutvecklingföretag delar liknande aspekter i de flesta fall som klientens relationer. I en mjukvaruutvecklingföretag utvecklas produkter eller lösningar åt klienter [27] medan i SOC övervakar medarbetarna produkter och system åt klienter [1]. Med det sagt, både mjukvaruutvecklingsföretag samt SOC har gemensamma syfte. Trots skillnaderna i arbetsinriktning delar både SOC och mjukvaruutvecklingföretag en gemensam grundläggande princip: att förstå och tillfredsställa klientens behov och förväntningar [27]. Detta är en central del av både SOC och mjukvaruutvecklingsföretag. Figuren nedan visar en illustration av hur mjukvaruutveckling och SOC har syn kring produkt.



Figur 2: Relation av mjukvaruutvecklingsföretag och SOC.

Från tidigare forskning gällande SOC och processmodeller har termen agil och SOC förekommit inom kort. En avhandling av S. Dushantha et al. [28] har använt agil arbetsmetod, nämligen hybrid scrum och kanban, för att utveckla en artefakt relaterad till en organisation av SOC-typen. En annan avhandling av O. Lindström [29] påpekar att SOC bör använda agil metod av den orsaken att hot kan eskalera in i incidenter snabbt. Detta är viktigt då SOC inte kan reagera snabbt inom strikta processmodeller [29]. En viktig aspekt inom detta är att stora organisationer inte använder agilt på grund av spridning av flera enheter och chefer [29].

Med det sagt, har tidigare forskning belyst att både SOC och mjukvaruutvecklingsföretag delar liknande aspekter, särskilt i relation till klienthantering. Båda typerna av organisationer strävar efter att förstå och tillfredsställa klientens behov och förväntningar. Forskning har också visat att agila metoder kan vara fördelaktiga för SOC, särskilt för att snabbt kunna reagera på hot och incidenter, även om stora organisationer ibland undviker agila metoder på grund av komplexiteten i deras struktur.

4 Metod och etisk analys

Detta avsnitt beskriver den metodologiska ansats som har valts för att besvara forskningsfrågorna. Avsnittet diskuterar de överväganden som gjorts vid val av metod, motiverar beslut och beskriver det planerade tillvägagångssättet, inklusive etiska överväganden. För att besvara FF1 och FF2, har studien valt en specifik organisation av SOC-typ som fallstudie och semistrukturerade intervjuer med en kvalitativ ansats. Till FF1 har det valts att studera utmaningar baserat på tekniska och organisatoriska som har inspirerats av en tidigare studie av B. Bruiners et al. [4]. Detta har valdes med hänsyn till att adressera utmaningarna i ett specifikt sammanhang än som generella utmaningar. Tekniska och organisatoriska utmaningar valdes också till att ta hänsyn mot den nuvarande processmodellen för organisationen. För att svara på FF1 behöver studien svar på de framstående utmaningarna inom såväl tekniska och som organisatoriska på den nuvarande processmodellen av den specifika organisationen av SOC-typen. För att kunna svara på FF2 kring vilka principer från agil och traditionell som kan implementeras i denna organisation, krävdes det att i första hand svara på FF1 samt ha en färdig bakgrund kring agil och traditionell processmodell.

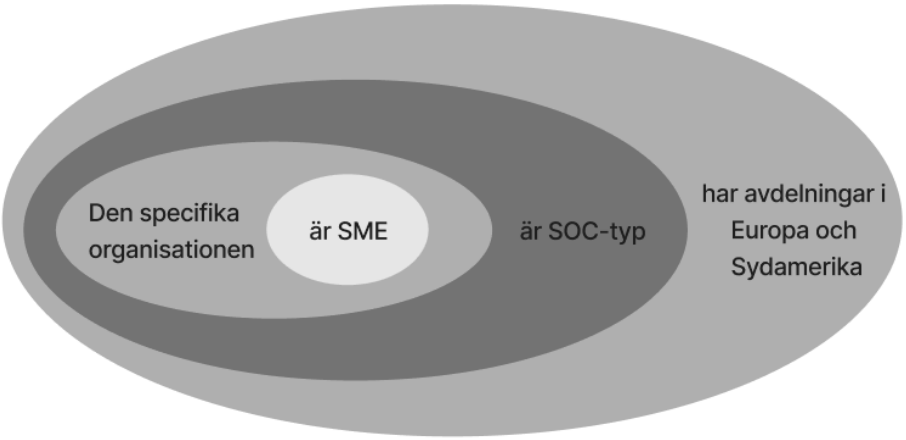
4.1 Metodbeskrivning

4.1.1 Fallstudie

Fallstudie är särskilt lämpliga när forskaren vill undersöka en samtida händelse inom dess verkliga kontext, särskilt när gränserna mellan fenomenet och kontexten inte är tydligt definierade [13]. Detta passade i stor utsträckning in i denna studie där det undersöks specifika tekniska och organisatoriska utmaningar inom en organisation av SOC-typ. Genom fallstudier produceras data som är nära människors erfarenheter [13], vilket med hjälp av intervjuer kommer att fördjupas i utmaningar med organisationen. Fallstudien ger också möjlighet att behandla komplexa situationer där det är svårt att studera en enskild faktor på en isolation [13]. Däremot kan fallstudier vara svårt och tidskrävande för att få tillgång till både människor och dokument [13].

Studien har valt den specifika organisationen av SOC-typ som fallstudie då den var representativ för andra SME inom samma sektor och var intresserad av att undersöka de datavetenskapliga arbetsmetoderna. Den organisation som gjorde kärnan i denna studie har sin verksamhet förlagd till flera kontor i både Europa och Sydamerika. Denna specifika organisation var bestående av 18 anställda som övervakar säkerhetsincidenter dygnet runt. De anställda arbetade från olika kontoren både i Europa och i Sydamerika. Kommunikation inom organisationen skedde både på kontoret och hemifrån, vilket gav en varierad arbetsmiljö som är idealisk för att studera olika arbetsprocesser och deras effektivitet. Denna organisation hade en nyanserad personalstruktur där individer innehar olika befattningar kopplade till specifika ansvarsområden [3]. Branschen för denna organisation var IT-säkerhet där de använde avancerade och automatiserade system för identifiering

och hantering av säkerhetsincidenter samt skapandet av larm. Organisationen arbetade nära traditionell arbetsmetod då arbetsflödet är linjärt, vilket i detta sammanhang innebär att säkerhetsincidenter övervakas och hanteras i ett sekventiellt flöde. Detta innebär att varje incident följer en fastställd process från identifiering till lösning, vilket ger insikter i de potentiella utmaningarna och ineffektiviteten i en sådan metod. Figuren nedan visar en överblick av fallstudien.



Figur 3: Överblick av fallstudien.

Valet av denna organisation av SOC-typen var strategiskt för studien av flera skäl:

- **Relevans till Forskningsfrågorna:** Organisationens fokus på IT-säkerhet och dess användning av både traditionella arbetsmetoder och verktyg gav en fullkomlig miljö för att studera tekniska och organisatoriska utmaningar i arbetsprocesser.

- **Villighet att delta:** Organisationens vilja att delta och ge insikter gjorde den till en ideal fallstudie. Detta innebär att studien hade tillgång till nödvändiga data och insikter för att sedan utföra en djupgående analys.

- **Representation av SME:** Som en SME inom IT-säkerhet representerade denna organisation en typisk struktur och arbetsmetod som kan vara generaliserbar till liknande organisationer. Detta gjorde studiens fynd mer relevanta och applicerbara på andra företag inom samma bransch.

- **Mångfacetterad personalstruktur:** Den mångfacetterade personalstrukturen med olika befattningar och ansvarsområden gav möjlighet att få insikter från olika perspektiv inom

organisationen, vilket var viktigt för att förstå de komplexa dynamikerna och utmaningarna som de står inför.

Med hänsyn till ovanstående punkter, har studien därför valt att studera denna organisation, specifikt när det presenterar SOC i världen. För att kunna studera den valda organisationen, valdes en lämplig metod för att åstadkomma med studiens forskningsfrågor, vilket kommer att presenteras i kommande avsnitt.

4.1.2 Semistrukturerade intervjuer

Genom semistrukturerade intervjuer ges det möjlighet att fördjupa sig i olika teman [13]. Semistrukturerade intervjuer är också flexibla vilket ger möjlighet att anpassa efter ordningen av frågorna [13]. En annan fördel är att respondenten har möjlighet att träffa forskaren och ge svar formellt framför forskaren [13]. Däremot är intervjuer tidskrävande och kan även vara artificiella synnerligen när intervjun spelas in [13]. På grund av dess fördelar, valdes därför semistrukturerade intervjuer - av den anledningen att de erbjuder en balans mellan struktur och flexibilitet, vilket möjliggjorde en djupgående utforskning av respondenternas upplevelser och perspektiv. Enligt J. B. Oates [13] tillåter även semistrukturerade intervjuer att ställa fördefinierade frågor samtidigt som det finns utrymme för följdfrågor och utforskning av nya teman som kan förekomma under intervjun. Detta var särskilt viktigt i denna studie, där studien försöker identifiera störst påverkade utmaningar inom SOC arbetsprocesser.

4.1.3 Kvalitativ ansats

Den kvalitativa ansatsen innebär insamling och analys av icke-numerisk data, såsom ord, bilder och ljud [13]. I denna studie kommer den kvalitativa ansatsen att tillämpas genom att analysera citat och andra verbala uttryck, med fokus på att värdesätta kvaliteten över kvantiteten. Denna metodologiska ansats var särskilt lämplig för studien då den möjliggör en djupgående förståelse av de detaljerade attityder och uppfattningar som är nödvändiga för att besvara forskningsfrågorna. Genom att prioritera kvalitativa data kunde studien fånga nyanserade insikter och komplexa fenomen som annars skulle kunna förbises i en kvantitativ ansats.

4.1.3 Alternativa Metoder

En alternativ metod för denna studie skulle vara att använda enkäter för kvantitativ analys, vilket skulle vara mer kostnadseffektivt än intervjuer då ingen transkribering skulle behövas [13]. Enkäter skulle möjliggöra insamling av data från ett större antal respondenter, vilket skulle ge en bredare bild av de tekniska och organisatoriska utmaningarna. Samtidigt finns det potentiella begränsningar med sådana enkäter. Det finns ingen garanti för att enkäterna skulle generera tillräckligt med svar inom den givna tidsramen för att möjliggöra en sammanställning av resultaten. Samtidigt skulle det vara utmanande att erhålla tillräckligt detaljerade svar genom enkäter som

behandlar kvantitativ analys. Enkäter tenderar att ge ytterligare svar och kan försumma nyanserna i respondenternas upplevelser och perspektiv [13]. Denna studie kommer dessutom att behöva mer kvalitativa data än kvantitativa för att kunna analysera och dra slutsatser baserat på text snarare än siffror. Eftersom studien kommer att identifiera största utmaningarna och behandla arbetsmetoder gentemot utmaningar inom SOC organisation, är det lämpligt att genomföra kvalitativa intervjuer för att samla in attityder och upplevelser om det nuvarande arbetssättet och dess utmaningar. Därför valdes intervjuer med kvalitativ analys som den föredragna metoden för denna studie. Intervjuerna möjliggör en djupare insikt i respondenternas upplevelser och perspektiv [13], vilket är avgörande för att förstå de komplexa utmaningarna och för att kunna formulera förbättringsförslag för SOC organisationens arbetsprocess. Genom att kombinera fallstudier och semistrukturerade intervjuer kan studien få en mer holistisk bild av problematiken och därmed ge mer välgrundade data för att besvara frågeställningarna.

4.2 Genomförande

För att genomföra en fallstudie samlade studien in data med hjälp av datainsamlingsmetoder som semistrukturerade intervjuer med sex anställda inom SOC organisationen enligt beskrivningen av B. J. Oates [13]. Dessa intervjuer skapade en flexibel struktur som kunde anpassas efter de rådande omständigheterna. Det har inneburit att intervjufrågorna inte nödvändigtvis ställdes in en förbestämd ordning, och att följdfrågor kunde uppstå under samtalets gång. Denna metod valdes då den möjliggör en djupare förståelse av respondenternas upplevelser och perspektiv, samt ger utrymme för upptäckter av nya insikter och mönster som kan vara relevanta för studiens syfte och frågeställningar.

4.3.1 Planering av intervjuer

Planeringen av intervjuerna utfördes parallellt med utarbetandet av kriterier som har hämtats från tidigare forskning [7], [8], [25], samt från organisationens dokumentation [1], [3]. Dessa kriterier omfattade tidigare identifierade utmaningar samt en beskrivning av hur SOC arbetade i helhet. Planeringen av intervjuerna involverade skapandet av protokoll och schemaläggning av intervjuerna under en veckas tid. Intervjufrågorna formulerades med hänsyn till de tekniska och organisatoriska utmaningarna som fanns i SOC:s nuvarande arbetsprocess. Kriterierna för typ av möte, dokumentationsmetoder och liknande hjälpte till att utforma intervjufrågorna. Genom en iterativ process justerades frågorna och förbättrades till den slutliga versionen. Den iterativa förbättringen av intervjufrågorna syftade även på att säkerställa deras relevans, anpassning efter tidsramen och att de var användbara under intervjun. I frågorna kom varierande tillvägagångssätt att användas, inklusive “vad”, “hur” och “varför”, för att få breda och relevanta svar. Under varje iteration sparkades underfrågor för att ytterligare styra och anpassa intervjun. Intervjuerna strukturerades för att inrikta på att identifiera både de tekniska och organisatoriska utmaningarna.

4.3.2 Kategori av tekniska och organisatoriska utmaningar

I samband med planeringen formulerades intervjufrågor baserat på följande tekniska samt organisatoriska utmaningar.

De tekniska utmaningarna inkluderade [4]:

- **Verktyg:** Utmaningar kring mjukvaru- och säkerhetsverktyg, särskilt verktyget som Splunk, ett säkerhetsverktyg för att övervaka säkerhetsincidenter, och verktyg för hantering av dokumentation som används inom organisationen.

- **Riktlinjer och policyer:** Utmaningar kring riktlinjer och policyer inom säkerhet samt för att säkerställa säkerhetsstandarder och anställda som följer dessa regler när de börjar jobba i organisationen.

De organisatoriska utmaningarna inkluderade [4]:

- **Planering:** Utmaningar med att planera och strukturera SOC operationer för att möta organisationens säkerhetsbehov på ett effektivt sätt.

- **Möten:** Utmaningar som gäller att effektivt planera och genomföra möten inom SOC där de diskuterar och löser säkerhetsrelaterade frågor och samarbetar med gruppen.

- **Dokumentation:** Utmaningar med att korrekt dokumentera säkerhetsincidenter och andra relevanta aspekter av SOC-verksamheten.

- **Samarbeten:** Utmaningar med att samarbeta och samordna med andra avdelningar och externa parter för att hantera och lösa säkerhetsincidenter.

- **Kommunikation:** Utmaningar med att kommunicera effektivt inom SOC och med andra avdelningar för att snabbt och korrekt hantera säkerhetsincidenter och informationsdelning.

- **Arbetsbelastning:** Utmaningar hur mycket arbete som tillsätts på en arbetsdag.

- **Kompetensutveckling:** Utmaningar för vidare möjligheter till att utbilda personal.

Baserat på de flesta av de ovan nämnda kriterierna har alla intervjufrågor färdigställts i slutet av planeringsfasen som visas i bilagor, *Bilaga 4: Intervjufrågor*. Utöver intervjufrågor, har en protokoll

skapats, som visas i bilagor, *Bilaga 5: Intervjuprotokoll*. Detta protokoll har använts för att informera respondenterna om syftet, användningen av data, samtycke till inspelning och sekretess. Intervjuerna ägde rum online via kommunikationsplattformen Teams med både kamera och ljud. Två av intervjuerna utfördes på svenska och resten på engelska. Den första intervjun planerades att genomföras som en pilotintervju för att sedan anpassa frågorna till kommande intervjuer. Pilotintevjun utfördes för att säkerställa att frågorna var passande för att erhålla en gynnsam svar. Efter genomförandet av en pilotintervju, fanns det inga behov av justering av intervjuer vilket gjorde att pilotintervjun användes som en del av datainsamlingen.

4.3.3 Tematisk analys

Efter genomförandet av intervjun, har den insamlade data analyserats tematiskt, där studien identifierade återkommande teman och mönster som studien redan hade definierat i planering: punkter med tekniska och organisatoriska utmaningar. Tematisk analys har rekommenderats av forskare som en metod för att identifiera, analysera och rapportera mönster (teman) inom data [30], [31]. Detta tillvägagångssätt gör det möjligt att systematiskt bearbeta intervjumaterialet och extrahera meningsfulla insikter som direkt relaterar till studiens forskningsfrågor. Enligt studien ovan tillåter tematisk analys utforskning av fenomenologi, vilket undersöker individers uppfattningar och förståelser av en företeelse eller situation genom intervjuer, berättelser eller observationer [30].

Intervjuerna transkriberades med hjälp av digitala verktyg som tal-till-text-konvertering och sedan manuellt granskades för att validera och säkerställa att data är korrekt. Efter transkriberingen genomfördes en verifieringsprocess där respektive respondent fick godkänna sina transkriberade svar. Detta steg var viktigt för att ge respondenterna möjlighet att rätta eventuella felaktigheter eller missförstånd i deras svar.

När godkännandet var klart, anonymiserades de transkriberade intervjuerna genom att ta bort respondenternas namn och annan personlig information. Därefter utfördes en tematisk analys inspirerad från V. Braun et al. [31] av intervjuerna att utföras i flera steg:

- **Initial kodning:** Varje transkription lästes noggrant igenom och initiala koder applicerades på textsegment som innehöll relevanta data. Detta har inneburit att denna studie markerade specifika passager som berörde tekniska och organisatoriska utmaningar samt potentiella förbättringsområden.

- **Identifiering av teman:** Efter den initiala kodningen granskades koderna för att identifiera återkommande mönster och teman. Dessa teman representerade de huvudsakliga utmaningarna och synpunkterna som samtliga respondenter har uttryckt.

Teman sorterades under de två huvudkategorierna: tekniska utmaningar och organisatoriska utmaningar.

- **Tabellering av data:** För att organisera och visualisera data strukturerades citat och teman i en tabell. Tabellen inkluderade information om respektive respondent, citat och tillhörande tema. Detta gjorde det möjligt att systematiskt sammanställa och analysera informationen. I bilagor, *Bilaga 6: Mall för citatfördelning*, visas mall för hur citaten strukturerades.

- **Analysera mönster:** De identifierade teman analyserades vidare för att förstå de underliggande mönstren och sammanhangen i respondenternas svar. Detta har inneburit att denna studie betraktade hur olika utmaningar relaterade till varandra och hur de påverkade den övergripande arbetsprocessen inom SOC organisationen.

- **Generering av insikter:** Baserat på den tematiska analysen, extraherades meningsfulla insikter som har varit relevanta till forskningsfrågorna. Detta inkluderade att identifiera både gemensamma och unika utmaningar samt föreslå möjliga förbättringsåtgärder.

4.3.4 Sammanfattning av genomförande

Genom en kvalitativ ansats, baserad på fallstudier och semistrukturerade intervjuer, undersöktes tekniska och organisatoriska utmaningar inom en specifik SOC organisation. Valet av denna SOC organisation motiverades av dess relevans för forskningsfrågorna, villigheten att deltaga och representativitet för SME inom IT-säkerhetssektorn.

Den metodologiska ansatsen möjliggjorde en djupgående utforskning av arbetsprocesser och utmaningar, vilket gav en rik och detaljerad förståelse för de faktorer som påverkade SOC-miljön. Genom att kombinera fallstudier och semistrukturerade intervjuer har studien samlat in omfattande data som har analyserats tematiskt för att identifiera återkommande mönster och komma fram med meningsfulla slutsatser. Denna ansats gav en fast grund för att svara på frågeställningar och bidra med värdefulla insikter till forskningsområdet.

4.3 Metoddiskussion

4.3.1 Metoddiskussion kring intervjuerna

Som det har nämnts tidigare genomfördes en pilotintervju som har godkänts och används i resultatavsnittet tillsammans med andra intervjuerna. Det är värt att överväga hur eventuella större justeringar i frågor kan ha påverkat resultaten. En annan aspekt att ha i åtanke är de olika rollerna som deltagarna hade i intervjun, vilket kan ha haft en inverkan på resultatens validitet och reliabilitet. Dessutom var transkriberingen av intervjuerna en utmanande process, särskilt med tanke på att intervjuerna genomfördes via Teams, vilket kan ha lett till att vissa ord eller uttryck inte fångade korrekt. För att säkerställa noggrannheten i transkriberingen skickades därför samtliga transkriberade intervjuer till respondenterna för godkännande. Genom intervjun online blev det även ytterligare utmanande för denna studie då fysiskt ögonkontakt med intervjupersonen har varit i mindre utsträckning. Det är också värt att observera att intervjufrågorna inte skickades i förväg till respondenterna för att undvika över förberedelse och för att uppmuntra till öppna och spontana svar, vilket är viktigt med tanke på studiens naturliga bidrag. Intervjuerna har gett skickliga och detaljerade resultat vilket större delen har varit bunden av hur organisationen jobbar. Förväntningarna skulle vara att utmaningarna skulle vara identifierade mycket tydligt, men verkade ge ganska ytligt från vissa respondenter.

4.3.2 Styrkor och svagheter

Datainsamlingen utgjorde en central del av studien, där studien samlade in data från både intervjuer och litteratur för den teoretiska bakgrunden. I bakgrundsdelen av denna studie identifierades forskning om användning av agila och traditionella metoder inom olika organisationer, främst inom mjukvaruutveckling, vilket är det område som är närmast och mest relevant för studiens syfte. Det bör noteras att det var begränsat med vetenskapliga studier som fokuserade specifikt på SOC och dess arbetsprocesser, vilket har omtalats tidigare. Av detta skäl, har denna studie haft svårt att utgå ifrån tidigare forskning kring samma ämne som denna studien behandlar. Å andra sidan, har semistrukturerade intervjuer gett detaljerade data som kunde i stort sett utgå ifrån studierna från mjukvaruutvecklingsföretag. Däremot finns det separat forskning som har varit relevant att ta upp, som utmaningar kring SOC, hur SOC jobbar, hur SOC:en kan förbättras utifrån tidigare forskning kring SOC och mjukvaruutvecklingsföretag som separata forskningsinriktningar.

Med det sagt, finns det inte direkt forskning när det gäller SOC [7], [2] i kombination med agil samt traditionell arbetsmetod. Även om det fanns en brist på datavetenskapliga studier om SOC, var det viktigt att använda närliggande litteraturer för att belysa relevanta aspekter av SOC:s arbetsprocess och jämföra dem med etablerade metoder inom agil och traditionell arbetsmetodik.

Genom att dra paralleller mellan liknande arbetsflöden och processer kunde studien fördjupa förståelsen för SOC:s specifika behov och utmaningar. Därför valde studien att inkludera forskning som bäst liknar SOC:s arbetsprocess och organisationer som tillämpar agila och traditionella arbetsmetoder. Det har därför också valts ytterligare databas som Google Scholar för att få så bred forskning som möjligt.

4.4 Etisk analys

4.4.1 Etisk aspekt kring intervjuerna

Enligt J. B. Oates [13] har människor som är involverade i forskningen rätt att bli behandlade på ett värdigt sätt. Detta inkluderar deras rätt att delta, dra sig ur, ge informerat samtycke, samt att deras anonymitet och sekretess skyddas. Denna studie har därför en skyldighet att anonymisera respondenternas namn, men även namnet på organisationen av SOC-typ för att upprätthålla konfidentialitet. De semistrukturerade intervjuerna som genomförs med anställda inom organisationen har också transkriberats och anonymiserats för att säkerställa att ingen personlig information bevaras. Efter att studien har slutförts, kommer även inspelningarna att raderas för att säkerställa sekretess ytterligare. Det är viktigt att varje anställd i organisationen måste godkänna den transkriberade intervjun och ge sitt samtycke till att informationen används för denna studie. Dessutom har intervjuerna endast spelats in av ljudformat efter samtycket av respondenterna.

4.4.2 Etisk aspekt kring forskningsmetodik

En annan viktig etisk aspekt är valet av forskningsmetod. Diskussioner har förts kring det mest lämpliga tillvägagångssättet för denna studie: att genomföra detaljerade intervjuer med organisationen eller att utföra en systematisk litteraturstudie om agila och traditionella modeller. Denna fråga har varit närvarande sedan studiens början och har inte varit ett enkelt beslut att fatta, särskilt med tanke på att fokus ligger på SOC, som utgör kärnan i denna forskning. Etiskt sett är det viktigt att överväga hur valet av forskningsstrategi påverkar nyttan av resultaten för organisationen och för andra forskare som kan använda denna studie. Valet att beskriva en bakgrundsstudie grundades på den begränsade tillgången på akademiskt relevant material om SOC i relation med agila och traditionella metoder. Å andra sidan har intervjuerna som sagt gett skickligt material som gör det möjligt att analysera baserat på den beskrivna teorin i bakgrundskapitlet.

4.5.3 Etisk aspekt kring presentation av studien

Ur ett etiskt perspektiv är det också viktigt att presentera innehåll och resultat på ett sätt som stämmer överens med både intervjuer och relevant forskning. För att säkerställa trovärdigheten hos de källor som används, har forskningsartiklarna granskats kritiskt innan de inkluderades i studien. Frågor som “Vem är författaren?”, “Är artikeln granskad?”, “Hur är artikeln skriven?” och “Vilka

referenser finns i artikeln?” har varit till hjälp för att kritiskt granska. Det fanns även andra forskningsartiklar som var relevanta för denna studie men som inte kunde användas på grund av dess otillgänglighet.

5 Resultat

Detta avsnitt presenterar resultaten från de semistrukturerade intervjuerna som inkluderar en detaljerad beskrivning av organisationen samt respondenternas synpunkter på de tekniska samt organisatoriska utmaningar. Resultaten har analyserats med hjälp av en tematisk analysmetod för att identifiera centrala teman och mönster. För att ge en tydlig kontext för resultaten, börjar studien med en utförlig beskrivning av organisationens bakgrund och verksamhet, vilket är avgörande för att förstå de utmaningar och lösningar som diskuteras i de efterföljande avsnitten. Resultaten i detta avsnitt bidrar till att besvara forskningsfrågorna och ge en djupare förståelse för hur organisationen fungerar i nuläget.

5.1 Organisationens bakgrund och verksamhet

Organisationen i fråga är en ledande aktör inom cybersäkerhet med ett globalt nätverk av SOC. Den analyserar och hanterar säkerhetsincidenter för ett brett spektrum av kunder, inklusive stora företag och offentliga institutioner [1]. Organisationen är uppdelad i flera nivåer av analytiker och specialister som arbetar tillsammans för att säkerställa en effektiv hantering av säkerhetsincidenter [1]. Enlig inciden chef samarbetar SOC tillsammans med andra externa IT-organisationer som bygger miljövaror och driver: "*Ja, egentligen med flera organisationer. Mest de som är IT-organisationer, det vill säga de som bygger miljövaror, de som driver med.*".

Organisationen av SOC-typ består av tre tekniska nivåer (L1, L2, L3) samt en chefsposition som ansvarar för strategiska beslut vid kritiska incidenter, enligt intervjun. Nivå 1 (L1) består främst av juniora analytiker som ansvarar för initial larmmottagning och triage av potentiella säkerhetsincidenter. Nivå 2 (L2) består av mer erfarna analytiker som hanterar komplexare incidenter och genomför detaljerad analys. Nivå 3 (L3) består av seniora säkerhetsanalytiker som specialiserar sig på avancerad incident och anpassning av övervakningssystem. Chefen för organisationen spelar en avgörande roll vid allvarliga incidenter genom att fatta beslut som kan påverka organisationens övergripande säkerhetsstrategi.

Den här uppdelningen i flera nivåer syftar till att möjliggöra en effektiv och systematisk hantering av säkerhetsincidenter, där varje nivå har klart definierade roller och ansvar. Detta ramverk speglar en strukturerad och hierarkisk modell som är central för hur organisationen fungerar och som har stor påverkan på hur tekniska och organisatoriska utmaningar hanteras.

5.2 Organisationens struktur och roller

SOC spelar en central roll i organisationens cybersäkerhetsstrategi genom att övervaka och hantera IT-infrastrukturen i realtid, dygnet runt. Huvudfunktioner inom SOC inkluderar kontinuerlig

övervakning av säkerhetshändelser, incidentrespons, och hantering av cyberhot [1]. Genom dessa funktioner kan SOC minska risker, öka säkerhetsmedvetenheten och hjälpa organisationen att förebygga och reagera effektivt på olika hot [1]. För att uppnå detta är SOC strukturerad med olika roller och nivåer som samverkar för att säkerställa en robust och effektiv säkerhetsorganisation.

5.2.1 Identifierade roller inom organisationen

Arbetsprocessen inom SOC involverar flera nyckelroller, som vardena bidrar till olika aspekter av säkerhetshanteringen:

- **Incident Chef:** Ansvarar för övervakning och hantering av medarbetarna, bedömning av incidentrapporter samt teknisk rådgivning. Incident Chefen spelar en avgörande roll i strategiska beslut vid kritiska incidenter [7].

- **Säkerhetsanalytiker:** Delas in i tre nivåer (L1, L2, L3), där L1-analytiker hanterar initiala larm genom triage och första undersökning, L2-analytiker utför djupare analys och hanterar mer allvarliga incidenter, och L3-analytiker är specialiserade på avancerad hot jakt och hantering av de mest komplexa incidenterna [7]. Mer om de nivåerna anges i “5.2.2 Arbetsprocessen av organisationen”.

- **Säkerhetskonsult:** Fokuserar på att forska kring och implementera branschstandarder och bästa praxis inom cybersäkerhet. Konsulten bidrar med expertis kring utveckling av säkerhetspolicys och procedurer [1], [7].

- **Säkerhetsarkitekt:** Ansvarar för planering och design av infrastrukturen av säkerhet. Säkerhetsarkitekten säkerställer att organisationens system är skyddade mot potentiella hot genom att utveckla och implementera robusta säkerhetslösningar [7].

- **Datavetare:** Samarbetar med säkerhetsgruppen för att samla in, normalisera och analysera data. Enligt intervjun spelar datavetaren en viktig roll i att omvandla rådata till användbar information som kan användas för att förbättra säkerhetsåtgärderna.

För att bekräfta att dessa roller stämmer enligt respondenternas beskrivning har studien även jämfört med andra studier som har beskrivit roller inom SOC [7]. Det tyder på att dessa roller har även bekräftats i tidigare forskning.

Intervjuer genomfördes med sex anställda som representerade deras olika roller: två junioranalytiker, två senioranalytiker, en incidentchef och en datavetare. Tabellen nedan visar en

sammanställning av respondenternas roller, inklusive deras specifika roller, arbetsuppgifter, erfarenhet och andra relevanta detaljer.

Respondent	Roll	Specifika roller och ansvar	Arbetsuppgifter	Erfarenhet
R1	Incidentchef	Strategiskt ledarskap och beslutsfattande	Övergripande hantering av kritiska incidenter	Mycket erfaren inom SOC
R2	Junioranalytiker	Första linjens analys och triage	Initial bedömning av larm, övervakning	Grundläggande till erfaren
R3	Senioranalytiker	Djupgående analys och tekniska åtgärder	Detaljerad incidentanalys, kontakt med kunder	Erfarna inom säkerhetsanalys
R4	Junioranalytiker	Första linjens analys och triage	Initial bedömning av larm, övervakning	Grundläggande till erfaren
R5	Senioranalytiker	Djupgående analys och tekniska åtgärder	Detaljerad incidentanalys, kontakt med kunder	Erfarna inom säkerhetsanalys
R6	Datavetare	Dataanalys och insiktsgenerering	Analyserar stora datamängder, stödjer incidenthantering	Expert inom dataanalys

Tabell 1: Överblick av respondenter.

5.2.2 Arbetsprocessen av organisationen

Arbetsprocessen inom en SOC kan delas in i tre huvudsakliga kategorier: förberedelse, övervakning och återställning [1], vilket presenterades i bakgrundskapitlet. Dessa processer utförs inom en hierarkisk struktur, vilket framgår både i intervjuerna med respondenterna och i tidigare forskning [7]. Resultatet av intervju om arbetsprocessen har samlats in genom frågor såsom:

1. *Skulle du kunna beskriva arbetsprocessen från start till slut? T.ex. ett typiskt arbetsflöde, hur ser det ut?*
2. *Finns det flera avdelningar som ni samarbetar med?*
3. *Can you describe how often you collaborate with other colleagues?*
4. *Can you describe how you handle documentation in SOC?*

Respondenterna beskriver arbetsprocessen genom att generalisera den i fyra nivåer:

- **Nivå 1:** Inkommande larm tas emot via säkerhetsverktyg som SIEM-system, exempelvis Splunk: "*tool, which is Splunk at the moment*". L1-analytiker genomför en så kallad *initialt triage*, det vill säga det första steget att initiera, och undersökning genom att bedöma larmens allvar och relevans. Detta görs genom att granska IP-adresser, analysera användarbeteenden och avgöra om larmen är falsk eller om de kräver vidare åtgärder. L1-analytiker samlar in grundläggande information om incidenten, inklusive enhetens historik och IP-adressens rykte, samt analyserar hashvärden för nedladdade filer för att bedöma deras legitimitet.

  Dessa steg utförs enligt dokumentation som finns för varje specifik incident eller larm: "*Det finns ju för varje larm vi får så finns det en dokumentation på hur du ska gå till väga".* I vissa fall, om dokumentation saknas, dokumenteras åtgärderna steg för steg under arbetets gång. Enligt en respondent: "*Så alla incidenter dokumenteras och man skriver det man har gjort och så, teknisk dokumentation typ... så här gör man när man trycker på knapparna".* Flera respondenter refererar till dokumentationsverktyg som används i arbetet, där de på frågan "*Can you describe how you handle documentation in SOC?*" nämner att de använder verktyget Confluence: "*we use Confluence, which is a product by Atlassian (company who also makes Jira). It is like a Wiki with databases.*" En respondent tillägger också: "*Most of the time, we use it as a Wiki or a FAQ".*

  Sammanfattningsvis utgör L1-analytikernas arbete grunden för den vidare hanteringen av säkerhetsincidenter [1]. Dokumentationen är särskilt viktig för L1-analytiker, eftersom många nyanställda börjar på denna nivå och förlitar sig på dokumentation för att vägleda dem i hanteringen av larm: "*This is helpful especially for new joiners...*". Om ett larm kräver ytterligare åtgärder, skapas ett ärende-ticket i systemet och eskaleras till L2-analytikerna för en djupare analys.

- **Nivå 2:** L2-analytiker genomför en mer detaljerad analys av incidenten. Enligt respondenterna kontaktar de andra avdelningarna och användaren direkt för att verifiera eller inhämta ytterligare information som behövs. I de flesta fall förlitar sig även L2-analytiker på dokumentation för att utföra tekniska åtgärder som lösenordsbyten och avbrytande av aktiva sessioner: "*Most of the times that we communicate with someone from*

another department and ask for specific information, we usually refer to the documentation". En respondent tillägger också: "*If a documentation is missing it will be added through the process of also resolving the issue that we contacted someone for in the first place.*" Detta visar på den centrala roll som dokumentation spelar inom SOC-arbetet.

Vid behov involveras L3-analytiker för att assistera både L1- och L2-analytiker: "*L3s help everybody if needed and tune alerts/cases or create new ones.*" Enligt respondenterna är L3-analytiker de experter som bidrar mest och ofta fattar beslut om ett specifikt larm ska stängas eller om ytterligare undersökning krävs: "*if they confirm it as a false positive, we adjust the priority from high to medium and close it out.*" Här tar seniora analytiker över och genomför en djupgående analys samt fattar beslut om vidare åtgärder.

- **Nivå 3:** På den högsta nivån (Nivå 3) ansvarar L3-analytiker för att hantera de mest komplexa och allvarliga säkerhetsincidenterna. Dessa analytiker besitter djup teknisk expertis, vilket gör att de kan fokusera på avancerade incidenter och anpassning av övervakningsregler för att förebygga framtida incidenter. Detta behov av att koncentrera sig på de mest kritiska aspekterna av säkerhetsarbetet understryks av att L3-analytiker ofta fördelar enklare uppgifter till L1-analytiker, vilket gör det möjligt för dem att fokusera på kärnuppgifterna: "*This way, they can focus on the core technical aspects of their work*." För att möjliggöra denna ansvarsfördelning hanterar L1-analytiker ofta sido projekt och uppgifter som, trots att de är enklare, fortfarande kräver betydande tid och uppmärksamhet: "*there are side projects where the L2 and L3 analysts rely on us to handle certain tasks that are relatively easier but still require some time.*" Genom denna arbetsfördelning kan L2- och L3-analytiker fokusera på mer strategiska och tekniskt krävande uppgifter, medan L1-analytiker bidrar genom att avlasta dem med mindre kritiska arbetsuppgifter.

- **Chefens involvering:** Vid kritiska incidenter involveras Incident Chefen för att fatta strategiska beslut och hjälpa till att säkerställa att incidenten hanteras effektivt. Respondenterna beskriver hur chefen kliver in vid dessa tillfällen för att leda hanteringen och garantera att incidenten hanteras på ett optimalt sätt: "*Our incident manager, [...], also takes a look at the queue and helps resolve the alerts.*".

Sammanfattningsvis kan arbetsprocessen inom en SOC förstås genom dess hierarkiska struktur där varje nivå har specifika ansvarsområden. L1-analytiker utför den initiala bedömningen och insamlingen av information, vilket utgör grunden för vidare arbete. L2-analytiker tar över för att genomföra en djupare analys och kan vid behov involvera andra avdelningar. L3-analytiker, som besitter den mest avancerade tekniska expertisen, hanterar de mest kritiska incidenterna och anpassar säkerhetsövervakningen för att förebygga framtida hot. Incident Chefen spelar en

nyckelroll i att leda hanteringen vid de mest kritiska incidenterna, vilket säkerställer att hela processen fungerar effektivt och att incidenterna hanteras optimalt.

5.2.3 Respondenternas syn på arbetsprocessen

Förutom en beskrivning av arbetsprocessen var respondenternas uppfattning om arbetsprocessen också viktigt att förstå, hur organisationen anser sig jobba idag (agil eller traditionell) och vad respondenterna tyckte om den nuvarande arbetsprocessen och förståelsen av andra arbetsmetoder. En fråga som formulerade på ett enkelt sätt som är baserat på beskrivning av arbetsflödet ställdes till respondenterna:

- *Vad tycker du om den nuvarande arbetsprocessen?*

Flera respondenter uppfattar att deras arbetsprocess är tydligt strukturerad och följd i en stegvis ordning, vilket är en traditionell sekventiell metod. Detta bekräftas av en respondent som beskrev arbetsflödet som *"Task wise, yeah, [...]"*, vilket antyder att processerna är noggrant definierade och att arbetsuppgifterna följer en förutbestämd sekvens.

Samtidigt finns det en medvetenhet hos somliga om att några element av agilt arbete kan finnas i den dagliga verksamheten, även om det inte har formellt identifierats som en agil arbetsmetod. En respondent förklarade: *"The way I follow the processes, the way I document the activity, the way I communicate with all the other teams is in some way agile."* Denna kommentar indikerar att även om SOC arbetsflöden inte formellt använder agila principer, finns det aspekter som iterativ kommunikation och samarbete som kan påminna om agilt arbetssätt, särskilt i samarbetet med andra team.

Det finns dock en viss osäkerhet bland andra respondenter kring arbetsmetodernas karaktär. Till exempel uttrycker en respondent förvirring över om de faktiskt arbetar agilt eller inte: *"Om jag får gissa så tror jag att vi jobbar agilt. Jag har väldigt dålig koll på det där."* Detta pekar på en bristande förståelse för arbetsmetodiken hos vissa anställda, vilket kan bero på att sekventiella eller agila principer inte är tydligt definierade eller kommunicerade i SOC kontext.

Flera respondenter betonade att agila metoder, i sin striktaste form, inte lämpar sig för den dynamiska och reaktiva naturen hos säkerhetsarbetet i en SOC. En senior säkerhetsanalytiker förklarade att arbetet inom SOC ofta handlar om att reagera på incidenter som uppstår plötsligt och oförutsägbart: *"You never know what alert shows up the next day."* Detta gör det svårt att använda agila principer som sprintplanering och regelbundna iterationer, eftersom arbetsflödet styrs av externa faktorer. Det kan dock finnas fall där en mer agil arbetsmetod är tillämplig, som vid kritiska incidenter, där flera personer arbetar parallellt på olika delar av ett ärende.

Generellt sett framkom att arbetsprocesser av SOC huvudsakligen är utformade kring individuellt arbete där varje person ansvarar för att hantera specifika ärenden eller larm. Detta förstärks av flera respondenter som noterade att agila principer, som kräver tät interaktion och skyndsamma återkopplade cykel, inte naturligt passar in i organisationens sätt att arbeta. En respondent nämnde att *"an alert is handled by a single person,"* vilket innebär att det inte finns tillräckligt med kollektiva moment för att fullt ut tillämpa agila metoder i det dagliga arbetet.

Trots dessa olika perspektiv verkar det finnas en allmän konsensus bland respondenterna om att arbetsprocesserna inom SOC är effektiva och välanpassade för det dagliga arbetet. Sammanfattningsvis kan det konstateras att även om agila metoder inte är fullt implementerade i SOC, finns det delar av arbetsflödet som påminner om agila principer enligt respondenternas beskrivning.

5.2 Resultat över utmaningar

I detta avsnitt fokuserar studien på de mest framträdande huvudteman i varje domän genom att presentera de relaterade underordnade teman och koder. Studien presenterar också citat från respondenterna för att belysa både positiva och negativa reflektioner kring de identifierade utmaningarna. När det gäller tekniska utmaningar har tre av sex respondenter nämnt verktyg som en mindre viktig utmaning. När det gäller organisatoriska utmaningar har fyra av sex respondenter betonade dokumentation och kommunikation som de största utmaningarna. Respondenterna påpekade ofta brister i den interna kommunikationen, vilket leder till ineffektivitet och missförstånd. Arbetsbelastning har därefter identifierades som en annan betydande utmaning enligt tre av sex respondenter. Utöver dessa huvudutmaningar finns även andra utmaningar som anses mindre viktiga, såsom planering, möten, kompetensutveckling och policyer. Det är särskilt intressant att en av de seniora respondenterna har betonat kompetensutveckling som en viktig och tidskrävande process.

5.2.1 Tekniska utmaningar

Verktyg, regler, riktlinjer och policyer

Organisationen använder idag flera olika verktyg för att hantera loggar och kommunicera effektivt. Några av de vanligaste verktygen inkluderar Splunk för logghantering och sökningar, Microsoft Teams för kommunikation, samt olika typer av brandväggar och Windows-loggar för att samla in och analysera data, inklusive IP-adresser, användarbeteende och andra kritiska loggar. En respondent anser att majoriteten av verktyget är bunden av Splunk och minoriteten på resten av arbetet: *"I would say that we're 90% of Splunk's activity and the rest of the jobs performed on it are just 10%."*. Dessa verktyg är centrala i det dagliga arbetet och hur de används framkom genom frågor ställda till respondenterna, till exempel:

- *Vilka utmaningar stöter du på i ditt nuvarande arbetssätt? Inklusive verktyg.*

Ett centralt tema som framkom i intervjuerna är att verktygen själva utgör en betydande utmaning för SOC-analytikerna. Flera respondenter lyfte fram verktyg som Splunk, brandväggar och Windows-loggar som nödvändiga, men samtidigt problematiska, eftersom de ibland är svåra att använda eller otillräckliga för vissa uppgifter. Exempelvis nämnde en respondent över att inte ha fullständig tillgång till verktyg som behövs för att lösa problem: "*För level 1 analys, så har du oftast inte tillgång till alla verktyg fullt ut och det kan vara så att jag vet om hur jag kan lösa ett problem men jag har inte verktyg till att göra det och det kan bli väldigt frustrerande*". Detta påvisar en tydlig utmaning där tillgången till och behörigheten för specifika verktyg är begränsad för L1-analytiker, vilket kan hämma deras förmåga att effektivt utföra sina arbetsuppgifter.

Vidare pekade en annan respondent på de utmaningar som uppstår vid distribution av nya verktyg eller mjukvaror, där dokumentation och konfiguration är kritiska men ibland bristfälliga. Denna utmaning framkom när respondenterna ombads att beskriva hur de hanterar sådana verktygsdistributioner: *"If we deploy a piece of software or tool it will be put to employers to document it and the different settings and then document the steps to follow for our version of the tool and draw a configuration.* Denna kommentar illustrerar den omfattande arbetsbörda som dokumentation kan utgöra, särskilt i en miljö där korrekt och uppdaterad dokumentation är avgörande för att upprätthålla effektiviteten i SOC.

När det gäller riktlinjer och policyer som påverkar SOC-arbetet, frågade studien:

- *Vilka begränsningar ser du inom SOC-miljön särskilt med avseende på regler, riktlinjer och policies?*

Svaren på denna fråga varierade. En respondent noterade kortfattat att regler och policyer visserligen påverkar arbetsprocessen, men utan att ge en djupare analys: "*Yes, it does affect the working process.*"

En annan respondent påpekade att regler och policyer är en del av den övergripande dokumentationen av infrastruktur som alla anställda måste acceptera vid anställning: "*So there's an infrastructure policies and compliance sort of documentation which everyone has to agree to upon joining the company.*". Denna till synes självklara aspekt av arbetsmiljön kan skapa hinder om policyerna är alltför restriktiva eller om de inte är anpassade till de specifika behov som uppstår i organisationen.

SOC-miljön är dessutom ofta en "stängd miljö", vilket kan försvåra informationsdelning och kommunikation, både internt och externt. Detta framkom när respondenterna ombads att diskutera utmaningar med informationsdelning: "*Ja, men det här är just stängt miljöer. Att vissa saker inte delas ut t. ex. dela ut av viss information.*". Den stängda miljön kan även påverka samverkan med andra avdelningar eller externa parter, vilket i sin tur kan leda till ineffektivitet och fördröjningar i arbetet.

En respondent, som är datavetare och arbetar med Splunk, beskrev utmaningar relaterade till förändringar i datastrukturer, såsom Windows-loggarnas format, vilket kräver kontinuerlig uppdatering av både dokumentation och datahantering: "*For example, the Windows data source changes a little bit of the format of the events every 3 months, and I need to update (not only the documentation—it is the most simple part—but also the parsing of the data).*" Denna återkommande förändring skapar utmaningar inte bara för datavetare, utan även för andra team som är bunden av att förstå och anpassa sig till dessa förändringar. En respondent uttryckte detta genom att beskriva svårigheten att förutse hur nya verktyg och system kommer att påverka SOC-arbetet: "*Sometimes we find that okay we're deploying a new type of firewall in 3 months or something for example. Then we're at the end of that deployment cycle rather than being in the early stages, because it helps us supply this well. Do you know how we're gonna use that tool? Can we use that tool? What benefit will it bring to the SOC and to the business?*"

Slutligen är det viktigt att notera att L1-analytiker har begränsad tillgång till vissa verktyg och behörigheter, vilket hindrar dem från att utföra vissa arbetsuppgifter. Endast seniora analytiker, såsom L2- och L3-analytiker, har fullständig tillgång till de resurser som krävs för djupgående undersökningar, som att analysera innehåll av e-post och köra vissa filer: *"As an L1 analyst, I don't have direct access to certain tools or permissions to run files. Only the L2 and L3 analysts have those privileges."* Denna begränsning speglar den tydliga ansvarsfördelningen inom teamet, där varje nivå har specifika roller och uppgifter baserade på deras kompetens och tillgång till resurser. Trots detta framstår verktyg som den största tekniska utmaningen inom SOC, även om de organisatoriska aspekterna också spelar en betydande roll.

5.2.2 Organisatoriska utmaningar

Dokumentation

Samtliga frågor ställdes under intervjutiden till respondenterna för att studera och få potentiella åsikter om dokumentation inom SOC:

- *Kan du beskriva hur ni hanterar dokumentation inom SOC?*
- *Vilka typer av information dokumenteras och under vilka faser? När dokumenterar ni händelser?*

Samtliga respondenter betonade vikten av dokumentation för att säkerställa effektiv hantering av incidenter och kunskapsutbyte inom gruppen. Dokumentationen hanterades genom både formella företagsdokument och flexibel dokumentation på plattformar som *Confluence* - en mjukvaruplattform där kunskap och samarbete möts.

Respondenterna framhöll också att dokumentation spelar en avgörande roll i hanteringen av larm och användningsfall. På Confluence kan gruppen hitta detaljerade arbetsflöden och instruktioner för hur de ska hantera och undersöka olika scenarier. Detta bidrar till att säkerställa en konsekvent och effektiv respons på incidenter: *"In SOC's Confluence you can find for example the workflow of the alerts, or even how to handle and investigate every Use Case we have etc.".*

En annan respondent påpekade också hur viktig dokumentationen är för att vägleda hur larm ska hanteras: *"Det finns ju för varje larm vi får så finns det en dokumentation på hur du ska gå till vägen."*. Dessa uttalanden framhåller att dokumentation är en kritisk komponent inom SOC, som inte bara fungerar som en handbok för specifika incidenter, utan också som en guide för att säkerställa en konsekvent arbetsmetod inom teamet.

- *Vilka utmaningar stöter du på i ditt nuvarande arbetssätt? Inklusive verktyg, möten, dokumentation och planering.*

Flera respondenter påpekade specifika utmaningar med dokumentation, utmaningar i samband med att hålla dokumentationen uppdaterad och relevant. En respondent nämnde att gammal dokumentation som inte längre är användbar ibland lämnas utan närvaro av uppdaterad status, vilket kan skapa ineffektivitet och förvirring: *"Utmaningen kan vara att kanske det finns gammal dokumentation som bara ligger där, som ingen underhåller."*. Detta indikerar att föråldrad dokumentation kan vara ett problem, och att det krävs ett bättre sätt att hantera dokumentationen för att säkerställa att informationen regelbundet uppdateras.

En annan viktig utmaning som lyftes fram var behovet av att upprätthålla en enhetlig standard i dokumentationen. En respondent påpekade att det ibland är svårt att få alla att följa samma mallar och riktlinjer, särskilt när olika medarbetare har varierande skrivstilar och dokumentationsförmågor: *"Documentation is one challenge, getting people to write the documentation sometimes it's a bit challenging except when it's got different writing styles and abilities so making sure that we get a consistent template together."*. Detta visar på behovet av tydliga riktlinjer och standardiserade mallar för att säkerställa att alla grupper inom SOC följer samma processer och arbetsflöden.

Vidare nämnde en annan respondent att dokumentationen i vissa fall inte uppdateras så frekvent som den borde, vilket kan påverka hur incidenter hanteras: *"Det skulle kunna vara dokumentationen, som kan förbättras på hur vi ska agera på en specifik incident eller dokumentationen på hur man ska göra för att det inte blir uppdaterat så frekvent som man kanske skulle ha gjort."*. Detta belyser vikten av att upprätthålla aktuell och korrekt dokumentation för att säkerställa att alla inom teamet vet hur de ska agera i olika situationer.

Med det sagt, har flera av respondenterna nämnt att dokumentation blir svårt när flera personer skriver på olika sätt, skrivstil och förståelse. Sammanfattningsvis betonar dessa insikter i dokumentationens viktiga roll inom SOC och de utmaningar som kan uppstå med att hålla dem uppdaterade och konsekvent. Det framgår att dokumentation inte bara är ett verktyg för att säkerställa effektiv incidenthantering, utan också en nyckelkomponent för kunskapsdelning och standardisering inom gruppen.

Samarbete och kommunikation

Samarbete lyfts inte lika starkt som dokumentation, men deras närvaro är viktig och anses vara både mindre utmanande och även mer utmanande enligt respondenterna. Samarbete mellan olika nivåer av analytiker i SOC anses vara en viktig del av arbetet, även om det ibland kan möta vissa utmaningar. Respondenterna var överens om att samarbete sker regelbundet, både inom teamet och över olika avdelningar, vilket är viktigt för att hantera säkerhetsincidenter effektivt.

- *Kan du beskriva hur ofta du samarbetar med andra kollegor? Och hur effektivt är det med samarbetet?*

Samtliga respondenter beskrev en stark samarbetskultur inom SOC. Samarbetet sker både på plats och på distans, beroende på arbetets karaktär och de verktyg som används. En respondent lyfte fram vikten av kontinuerligt samarbete och förklarade att det är vanligt att samarbeta med kollegor flera gånger i veckan, ofta i samband med olika uppdrag och projekt: "*Overall, we collaborate regularly for one or two days each week on various assignments and projects.*" Detta samarbete

sträcker sig över de olika nivåerna av analytiker – L1, L2 och L3 – och med incidenthantering, vilket underlättar kunskapsdelning och snabbare lösningar på incidenter.

En annan respondent förtydligade vikten av att arbeta tillsammans för att uppnå resultat och att samarbete är nödvändigt i SOC: "*Du klarar det ju inte utan att jobba med andra.*" Denna kommentar understryker hur central samverkan är för att SOC ska fungera effektivt, då det sällan är möjligt att hantera alla uppgifter på egen hand.

- *Vilka utmaningar stöter du på i ditt nuvarande arbetssätt? Inklusive samarbete och kommunikation.*

Trots att samarbete är en viktig del av arbetet, finns det också utmaningar kopplade till detta. En av utmaningarna som lyftes fram var att vissa kollegor ibland prioriterar andra uppgifter, vilket kan leda till att samarbetet försenas: "*Det funkar bra, men ibland gör folk något annat, prioriterar något annat och då kan det ta väntetid.*" Detta visar på att även om samarbetet i grunden fungerar väl, kan individuella prioriteringar påverka teamets förmåga att hantera vissa uppgifter i tid. Att hantera dessa prioriteringskonflikter kan därför vara en utmaning.

Flera respondenter identifierade utmaningar relaterade till kommunikation, med återkommande tema av språkbarriärer. Trots att engelska är det huvudsakliga språket inom företaget, noterade en respondent att skriftlig kommunikation på engelska ibland kan leda till missförstånd: "*Ett problem som jag kan säga kan ju vara att kommunikationen är så skriftlig med engelskan.*" Detta pekar på att vissa medarbetare inte har engelska som modersmål, vilket kan påverka förståelsen och därmed samarbetet inom teamet.

Vidare nämnde en annan respondent att de flesta larm som SOC hanterar kommer från externa källor, vilket innebär att kommunikation med andra användare och avdelningar är nödvändig för att lösa problemen: "*But since most of the alerts reach us from outside of SOC and we need to talk with other people/users to mitigate most of the issues, there are some communications issues.*" Detta belyser vikten av tydliga kommunikationskanaler mellan SOC och övriga organisationen. När kommunikationen brister, särskilt med externa team, kan det försvåra och fördröja incidenthanteringen, vilket innebär att arbetsflödet blir mindre effektivt.

Distansarbete har också introducerat nya utmaningar. En respondent påpekade att distansarbete kan göra det svårare att bygga relationer och förstå företagskulturen, särskilt för nya medarbetare: "*[...] remote work did pose some challenges, especially when I was new to the company [...]*". Denna observation lyfter fram hur distansarbete kan försvåra integrationen för nyanställda och göra det svårare att etablera ett starkt samarbete tidigt. Samtidigt pekade flera respondenter på vikten av att

ha strukturerade utbildnings- och onboarding-processer för att underlätta för nya medarbetare att komma in i arbetet och teamet, vilket kan mildra dessa utmaningar.

Trots dessa utmaningar framkom det att samarbetet inom SOC generellt fungerar väl, särskilt med hjälp av kommunikationsverktyg som Teams

Kompetensutveckling och arbetsbelastning

Behovet av kontinuerlig kompetensutveckling och utbildning är avgörande i alla organisationer, särskilt inom säkerhetsincidenthantering. Inom SOC är det en nödvändighet för att möta de ständigt föränderliga kraven och utmaningarna. För att undersöka hur kompetensutveckling och utbildning hanteras i SOC idag, ställdes följande fråga till respondenterna för att få deras åsikter:

- *Hur ser möjligheten ut för kompetensutveckling?*

Samtliga respondenter pekade på vikten av kontinuerlig förbättring inom dessa områden för att skapa en effektivare arbetsprocess som gynnar alla inom gruppen. Det kan också indikera att anställda inom organisationen upplever att kompetensutveckling och planering är utmanande med den nuvarande arbetsprocessen.

Flera respondenter betonade att det finns möjlighet till strukturerad utbildning och certifiering, där personal kan vidareutveckla sin kompetens: *"Det finns en kurs som man kan certifiera sig och ha olika inriktningar"* och *"Det går en gång per år."* Denna form av regelbunden utbildning, som erbjuds av tredjepartsleverantörer, ger personalen möjlighet att specialisera sig på olika verktyg och områden inom säkerhetsarbetet, vilket är en viktig del i att möta de tekniska kraven i SOC. En respondent noterade också vikten av att träning är både kostnadseffektiv och strategisk: "*Generally it is cheaper and more economical to train and pay the employees well rather than pay to replace the employees every year"*

Trots att möjligheter till utbildning förekommer, finns det utmaningar särskilt när det gäller att introducera nya medarbetare och ge dem rätt verktyg och kunskap för att arbeta effektivt. En respondent uttryckte att onboarding och träning kan vara en långsam process och påpekade att det krävs tillgång till dokumentation och tips för att snabbt förstå processer: *"onboarding and training process [...] get access to the documentation so you can understand what the processes and how things get done."* Detta tyder på att det nuvarande systemet för introduktion av nya medarbetare inte alltid är tillräckligt snabbt eller strukturerat.

En annan utmaning som lyftes fram var att träna nya medlemmar i gruppen, särskilt i samband med distansarbete: *"Training new members of staff is [...] a bigger bit of a challenge especially with*

remote work." Detta pekar på att distansarbete, som blivit allt vanligare, försvårar utbildningsprocessen då det kan vara svårare att överföra praktiska kunskaper och ge stöd med handledning på distans. Även om mentorprogram förekommer, där L1-analytiker tilldelas mentorer från högre nivåer (L2 och L3), framkommer det att dessa program skulle även kunna förbättras för att bättre möta behoven av kunskapsöverföring och personlig utveckling.

- *Hur planerar och fördelar ni arbetet inom teamet? Finns det några utmaningar kring detta då?*

Respondenterna nämner arbetsbelastning som svar på frågan, flera respondenter nämner utmaningar som tidsbrist och behovet av att förbättra prioriteringen av ärenden. *"[...] det är en överbelastning på arbetet"* beskrev en respondent, och noterade att när arbetskön blir för stor, med ett högt antal larm (t.ex. 150-200 larm), behöver gruppen söka hjälp från L2- och L3-analytiker för att avlasta arbetsbördan. Detta understryker att det nuvarande arbetsflödet inte alltid räcker till för att hantera den stora mängden larm, vilket påverkar effektiviteten och i förlängningen incidenthanteringen. En respondent beskriver att *"If the queue becomes unmanageable, with a high number of alerts like 150 or 200, we seek assistance from the L2 and L3 analysts."*

Språkbarriärer inom den globala organisationen lyfts också som en möjlig utmaning, där verksamheten är verksam i flera regioner och team ibland kan ha svårt att stödja varandra på grund av språkförbistring: *"language is sometimes a challenge [...] some teams can't support that and they speak in a local language."* Detta indikerar att även om affärsengelska används, kan språkproblem i internationella team hindra effektivt samarbete, särskilt i situationer där snabb kommunikation är avgörande.

6 Analys och diskussion

Detta avsnitt presenterar analys av studiens resultat. Analysen kommer först att utföras genom att noggrant kolla på utmaningar i relation med respondenternas syn på de utmanande aspekterna. Därefter kommer respondenternas syn av arbetsprocessen att analyseras. I samband med utmaningar samt arbetsprocess, kommer teorier att presenteras. Det finns teorier som både bekräftar och urskiljer för att kunna tolka resultaten. Till sist presenteras diskussionen för att öppna upp tankar och funderingar som kan leda till slutsatser.

6.1 Analys

Tabellen nedan visar en fördelning av respondenternas syn på utmaningar baserat på resultatet. Baserat på de viktiga citat från resultatet, placerades varje respondent inom 3 teman: ingen utmaning, mindre utmanande och mer utmanande. Citatens intryck av ord avgör till vilket tema som respondenternas syn klassificerades. Efter att kvalitativt uppdela respektive respondenter i de tre teman, visas vilka tekniska respektive organisatoriska utmaningar som har blivit ett framstående intryck.

	Ingen utmaning	**Mindre utmanande**	**Mer Utmanande**
Tekniska utmaningar			
Verktyg	R1	R3, R5, R6	R2, R4
Riktlinjer och policyer	R1, R3, R5	R2, R4, R6	
Organisatoriska utmaningar			
Planering och möten	R1, R3, R5, R6	R2, R4	
Dokumentation		R1, R3	R2, R4, R5, R6
Samarbete och kommunikation	R1	R2, R5, R6	R3, R4
Kompetensutveckling	R1, R2, R3, R5	R4, R6	
Arbetsbelastning		R1, R3, R5	R2, R4, R6

Tabell 2: Överblick av respondenternas syn på utmaningar.

- **Verktyg, riktlinjer och policyer**: Utmaningar kring verktyg har varit utmanande bland respondenterna. Enligt teorin [7] så kan automatiska verktyg hantera välkända attacker som kan underlätta arbetet. Å andra sidan, har teorin [7] också bekräftat tillsammans med intervjun att verktyg är utmanande då de inte har tillgång till alla verktyg. Detta är något som är förknippad med arbetsbelastning då personal inte har tillgång till de verktyg som

kan underlätta arbetet. Vad gäller riktlinjer och policyer, kan rutinmässig analys minska missbruk av policyer [26]. Faktumet är att enligt intervjun så är det utmaning med riktlinjer och policyer då de måste följas. Dock anses riktlinjer och policyer ingen stor utmaning.

- **Planering och möte**: På samma sätt har planering och möte inte varit en särskilt stor utmaning enligt resultatet förutom att det är svårt att planera för det larm som kommer slumpmässigt. Likvida har det inte belysts särskilt utmaningar inom tidigare forskning kring SOC [7], [8], [2], men det har däremot beskrivits förekomsten av detaljerad planering och olika mötestillfällen inom traditionell och agil metod [22].

- **Dokumentation**: En av de mest framträdande utmaningarna är dokumentation, vilket framgår tydligt från intervjuerna. Detta överensstämmer med teorier om existerande utmaningar kring dokumentation eller logghantering i SOC [26]. Dokumentation är en kritisk komponent inom SOC, där effektiv insamling, analys, dokumentering och lagring av loggdata är avgörande för att identifiera och hantera säkerhetsincidenter [26]. Denna process är ofta tidskrävande och komplex, vilket gör dokumentation till en betydande utmaning, enligt respondenterna. Dessutom betonar andra teorier [5], [15] att dokumentation inom till exempel vattenfallsmetoden kan vara tungrodd och byråkratisk, vilket ytterligare förstärker problemet kring dokumentationen.

- **Samarbete och kommunikation**: En annan viktig utmaning är samarbete och kommunikation, särskilt med hänsyn till kommunikation kring distansarbete och språkbarriärer inom gruppen. Sammarbetet funkar bra enligt respondenter, dock ställer kommunikationen en utmaning på samarbetet. Enligt respondenterna kan distansarbete leda till känslor av isolering och svårigheter att upprätthålla en effektiv kommunikation, samtidigt betyder respondentens svar att det kan påverka gruppens sammanhållning och produktivitet. Dessutom kan språkbarriärer skapa missförstånd och försvåra samarbetet, särskilt i multinationella grupper där medlemmarna har olika modersmål. Teorin bekräftar att samarbete och kommunikation är väsentliga inom gruppen [7], men inte på den graden att språk eller distansarbete påverkar som det har belysts i intervjun. Forskning visar att tydlig och frekvent kommunikation är avgörande för att övervinna dessa utmaningar och skapa starka grupper [7], även när medlemmarna arbetar på distans.

- **Kompetensutveckling**: Kompetensutveckling har både visat möjlighet att utbilda personal men också på mindre bristande områden enligt intervjun. Teorin har inte visat utmaningar kring kompetensutveckling [7]. Dock har teorin visat att en bra kompetensutveckling inom SOC kan göra personer mer professionella att hantera uppkommande larm [7].

- **Arbetsbelastningen**: Arbetsbelastningen är en utmaning som flera respondenter har betonat. Teorin betonar att metoder som Lean Development kan minimera processerna och fokusera på åtgärder [4]. Som en uppkomst av arbetsbelastning visar däremot teorin att det finns brist på automatiserade verktyg [7]. I jämförelse med intervjuerna har arbetsbelastningen å andra sidan inte identifierats som en orsak till bristen på automatiserade verktyg, utan intervjuerna har belyst existensen av automatiserade verktyg som effektiviserar organisationens hantering av incidenter.

Enligt intervjun har samtliga respondenter även beskrivit arbetsprocessen, det vill säga de olika nivåerna som Nivå 1, Nivå 2, Nivå 3 och Chefen. Resultatet från intervjun har visat att de flesta respondenterna var omedvetna till vilken av processmodell agil eller traditionell den nuvarande organisationens arbetsprocessen tillhör. Inom tidigare forskning [11], [12], [4] har det inte visat ett sådant fall då personal har varit omedvetna om deras process. Detta betyder att organisationen inte har en förutbestämd arbetsprocess som definieras varken agil eller traditionell som tidigare forskning kring mjukvaruutvecklingsföretag har angivit [11], [12], [4]. Organisationen har ett eget arbetsprocess med olika nivåer som det har visat i tidigare forskning kring SOC [7]. Dock har studien av Z. Bakalova et al. [27] visat att det inte finns en klar gräns mellan agil och traditionellt arbetssätt. Tolkningen kan i detta fall ligga att organisationen arbetar traditionellt på omedvetet sätt. Organisationens arbetsprocess har beskrivits på liknande sätt som beskrivningen av den traditionella principen. Skillnaden är att organisationen jobbar stegvis och inte projektvis. Å andra sidan, har en annan teori har även belyst brist på akademiska artiklar som fördjupar förståelsen av SOC, särskilt när det gäller beskrivning av arbetsmetoder [7]. Detta är dock något som sammanträffar med resultatet av intervjun om omedvetenhet kring arbetsmetoden agil och traditionell processmodell. Samtidigt anges det att SOC bör använda agil metod av den orsaken att hot kan eskalera in i incidenter snabbt [29]. Tidigare studier kring detta har även visat att många av mjukvaruutvecklingsföretag började använda sig av agila metoder [11], [12], [4] och andra säkerhetstjänster började använda traditionella metoder i kombination med agila metoder [4]. Detta öppnar mer diskussionen kring vilket princip från agila och traditionella metoder som kan ge en möjlig integration för organisationens nuvarande arbetsprocess.

6.2 Diskussion

Dokumentationen har varit en viktig aspekt inom organisationen enligt de flesta av respondenterna. De flesta respondenterna har nämnt att gamla dokumentation behöver uppdateras och det är utmanande idag. Respondenterna betonar dokumentationens vikt i sitt dagliga arbete då den ger vägledning för att hantera olika typer av larm som kommer in i organisationen. För ett sådant tillstånd, är traditionella principen om dokumentationshantering med UML verktyget [21] en möjlig väg till förbättring i organisationens dokumentation. Dock är UML anpassad för dokumentation kring systembeskrivning snarare än dokumentation av incidenter. Detta öppnar upp fler diskussioner kring andra principer som förbättring.

Resultatet från intervjun kring planering beskriver inget väldefinierad planering då gruppen åtgärdar incidenter som kommer vid olika tillfällen. Detta kan göra saken svår att planera framåt. Dock har intervjun belyst att planering kan existera vid korta tillfällen då ett larm ska lösas och hur i sådana fall. Trots att det finns olika typer av möten, upplever vissa respondenter internkommunikationen på grund av språklig brist och mellan avdelningar i olika geografiska områden. Som ett förslag hade organisationen kunnat införa fler kompetensutvecklingsprogram för att utöka kunskaper inom språk såväl som hantering av verktyg och dokumentation. Som ett annat förslag hade flera muntliga möten förmodligen varit passande. För ett sådant tillstånd är agil metoder passande och flexibla med samarbete och kommunikation. Scrumban är ett av agila metoder som är effektiva [4]. Studierna indikerar att intern kommunikation och medarbetare kan förbättras genom att använda agila metoder såsom Scrumban då metoden håller regelbundna möten [4]. Genom att ha flera möten blir det tydligare och enklare att kommunicera med varandra och hantera uppgifter mer effektivt och vara mer produktiva [28].

Verktyget har också varit en utmanande aspekt av vissa respondenter då alla verktyg inte var tillgängliga. Trots att organisationen använder Splunk som primära verktyg av incidentövervakning kan fler möjligheter av verktyg ges för optimering av arbetsprocessen. Den agila metoden kanban optimerar processer genom att visualisera arbetsflödet [9]. Detta görs med hjälp av ett system där arbetsuppgifter representeras som kort på en tavla, som visar uppgifter i olika stadier som "Ej påbörjade", "Pågående" och "Klar" [9], [18]. Denna kanban liknar i stort sett beskrivningen av organisationens arbetsprocess där incidenter placeras i en kö för att bli åtgärdade. Principen av kanban-board kan hjälpa organisationen att tydligt se vad som behöver göras och fördelar arbetet på ett strukturerat sätt. Organisationen har stand-up möten idag enligt intervjun, vilket är applicerbart med scrum möten. Med det sagt, skulle principen av att ha fler möten enligt Scrumban förbättra internkommunikationen. Endast scrum i sin helhet kan dock inte passa då scrum är avsedd för komplexa projekt [4]. Därför kan kombinationen av principen av fler scrum-möten samt kanban-board leda till implementering till organisationens arbetsprocess.

Genom att förbättra samarbete och kommunikation i grupp kan det leda till förbättring av arbetsbelastningen som är en annan betydande utmaning. Principen från Lean Development kring snabb åtgärd [4] kan också bli en väg till implementering i organisationens arbetsprocess. Det är viktigt att processer och åtgärder utförs snabbt. Dock kan kvaliteten hastigt minska då åtgärderna görs snabbt. Agila metoder som Dynamic Systems Development Model (DSDM) och Adaptive Software Development (ASD) kring principen flexibilitet och kundcentrerad iteration [4] kan även bidra till en implementering i organisationen. Begränsningen kan bidra till att de är mest anpassade efter projekt, vilket gör det mindre passande för organisationen. På samma sätt är Crystal och Feature-Driven Development (FDD) mindre passande då metoderna betonar projektarbete samt dokumentation av funktionslista [4]. Traditionella metoder som Unified Process (UP) och spiralmodellen kan också bli mindre passande då metoderna utförs på ett iterativt och inkrementellt sätt [21].

Faktumet är att traditionella metoder kan ibland leda till överbelastning på grund av strikta hierarkier och fasta roller, vilket kan begränsa flexibiliteten [5]. Det som respondenterna förklarade i intervjun var att det finns situationer där de återvänder till tidigare steg i arbetet, vilket inte heller är strikt. Situationen har varit när incidentanalytikerna behövde skicka tillbaka larm åtgärd från nivå 2 (L2) till nivå 1 (L2). Agila metoder däremot, med sin betoning på självorganiserande grupper och anpassningsbarhet, kan hjälpa till att fördela arbetsbelastningen mer jämnt och minska stress [5], [14]. Trots att empiriska studier har visat väg till hybrid val av metoder i olika organisationer [5]-[22]-[9]-[10]-[20], är det däremot inte liknande i detta fallstudie med organisationen. Organisationens arbetsprocess anses inte kunna implementera antingen en helt agil metod eller traditionell metod. Detta eftersom det finns ett gräns mellan projektarbete och ett gräns mellan åtgärder av incidenter. Därför kan endast principer från agila och traditionella metoder bli en möjlighet att integrera med organisationens arbetsprocess, vilket har koppling till studiens syfte och frågeställning. Genom dessa diskussioner, kan slutsatser presenteras till vad studien kom fram till.

7 Slutsatser och vidare forskning

Bidraget med denna studie har varit att inrikta mot en specifik organisation av SOC-typ för att först identifiera specifika utmaningar kring arbetsprocessen och sedan vilka principer från olika processmodeller som agil och traditionell metodik från mjukvaruutvecklingsföretag kan implementeras. Resultaten av denna studie belyste olika utmanande aspekter kring ett tekniskt och organisatoriskt perspektiv. Genom analyser och diskussioner med teorier har potentiella slutstserna kunnat tas fram.

7.1 Svar till FF1

FF1: Vilka tekniska respektive organisatoriska utmaningar har ett framstående intryck på en specifik organisation av SOC-typ med den nuvarande processmodellen?

- Inom tekniska utmaningar är verktyg den utmanade aspekten medan inom organisatoriska utmaningar är dokumentation, kommunikation samt arbetsbelastning som de största påverkan för organisationens arbetsprocess. Valet av just dessa utmaningar belyser vikten av intervjuerna med en kvalitativt ansats.

7.2 Svar till FF2

FF2: Vilka principer från agil och traditionell processmodell från mjukvaruutvecklingsföretag kan implementeras på den nuvarande processmodellen för en specifik organisation av SOC-typ?

- Den främsta principen som kan implementeras är Scrumban’s regelbundna möten samt Kanban's board för att ha en överblick av aktuella, pågående och avslutande incidenter.

7.3 Vidare forskning

För vidare forskning föreslås det att utforska *hur* implementationen av Scrumban eller Kanban kan utföras. Slutligen kan vidare forskning behandla flera fallstudier, där framtida forskningen kan jämföra agila och traditionella metoder gentemot olika typer av organisationer av samma SOC-typ. Genom att utforska dessa möjligheter kan framtida forskning bidra med riktlinjer och praktiska lösningar för att övervinna de utmaningar som organisationen av SOC-typen står inför idag.

Referenser

[1] M. Scapicchio, A. Downie, M. Finio, "*What is a Security Operations Center (SOC)?,"* i *IBM*. 2024. [Online]. Tillgängligt: https://www.ibm.com/topics/security-operations-center (Hämtad: 25 Januari 2024).

[2] P. Jacobs, A. Arnab, B. Irwin, "*Classification of Security Operation Centers*," i Information Security for South Africa, Johannesburg, South Africa, 2013, ss. 1-7, doi: 10.1109/ISSA.2013.6641054.

[3] Commission of the European Communities, "*Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422) (Text with EEA relevance) (2003/361/EC),*" Official Journal of the European Union, vol. L124, pp. 36-41, May 2003. [Online]. Tillgängligt: http://data.europa.eu/eli/reco/2003/361/oj (Hämtad: 25 Januari 2024).

[4] B. Bruiners, O. Jokonya, "*Factors Influencing the Adoption of Agile Methodology within SMEs in Cape Town*," i International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Vanderbijlpark, South Africa, 2019, ss. 1-8, doi: 10.1109/IMITEC45504.2019.9015886.

[5] N. Yahya, S. S. Maidin, "*The Waterfall Model with Agile Scrum as the Hybrid Agile Model for the Software Engineering Team*," i 10th International Conference on Cyber and IT Service Management (CITSM), Yogyakarta, Indonesia, 2022, ss. 1-5, doi: 10.1109/CITSM56380.2022.9936036.

[6] A. Sinha, P. Das, "*Agile Methodology Vs. Traditional Waterfall SDLC: A case study on Quality Assurance process in Software Industry*," i 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2021, ss. 1-4, doi: 10.1109/IEMENTech53263.2021.9614779.

[7] M. Vielberth, F. Böhm, I. Fichtinger, G. Pernul, "*Security Operations Center: A Systematic Study and Open Challenges*," i IEEE Access, vol. 8, ss. 227756-227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

[8] F. D. János, N. Huu Phuoc Dai, "*Security Concerns Towards Security Operations Centers*," i IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2018, ss. 000273-000278, doi: 10.1109/SACI.2018.8440963.

[9] A. Mishra, S. Abdalhamid, D. Mishra, S. Ostrovska, "*Organizational issues in embracing*

Agile methods: an empirical assessment," i International Journal of System Assurance Engineering and Management, vol. 12, ss. 1420–1433, Okt. 2021, doi: 10.1007/s13198-021-01350-1.

[10] E. C. Conforto, F. Salum, D. C. Amaral, S. da Silva, L. de Almeida, "*Can Agile Project Management Be Adopted by Industries Other than Software Development?*," i Project Management Journal, vol. 45, nr. 3, ss. 21-34, Jun. 2014, doi: 10.1002/pmj.21410.

[11] K. Sureshchandra, J. Shrinivasavadhani, "*Moving from Waterfall to Agile*," i Agile 2008 Conference, Toronto, ON, Canada, 2008, ss. 97-101, doi: 10.1109/Agile.2008.49.

[12] E. Kim, S. Ryoo, "*Agile Adoption Story from NHN*," i IEEE 36th Annual Computer Software and Applications Conference, Izmir, Turkey, 2012, ss. 476-481, doi: 10.1109/COMPSAC.2012.83.

[13] B. J. Oates, *Researching information systems and computing*, 1st ed. London: SAGE, 2006.

[14] F. L. Ribeiro, M. T. Fernandes, "*Exploring agile methods in construction small and medium enterprises: a case study*," i Journal of Enterprise Information Management, vol. 23, nr. 2, ss. 161-180, Feb. 2010, doi: 10.1108/17410391011019750.

[15] R. Bin-Hezam, A. Bin-Essa and N. F. Abubacker, "*Is the Agile Development Method the Way to Go for Small to Medium Enterprises (SMEs) In Saudi Arabia?*," i 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 2018, ss. 1-6, doi: 10.1109/NCG.2018.8592990.

[16] Sommerville, Ian (2015). Software Engineering, Global Edition, 10:de upplagan, Pearson.

[17] W. Daoudi, K. Doumi, L. Kjiri, "*Adaptive Enterprise Architecture: Towards a model*," i Proceedings of the 10th International Conference on Information Systems and Technologies (ICIST '20). Association for Computing Machinery, New York, NY, USA, 2021, ss. 1-7, doi: 10.1145/3447568.3448539.

[18] C. C. Huang, A. Kusiak, "*Overview of Kanban systems*," i International Journal of Computer Integrated Manufacturing. 1996. vol. 9, nr. 3, ss. 169-189, doi: https://doi.org/10.1080/095119296131643

[19] R. Mokhtar, M. Khayyat, "A Comparative Case Study of Waterfall and Agile Management," i SAR Journal, Jeddah, Saudi Arabia, 2022, vol. 5, nr. 1, ss. 52-62, doi: 10.18421/SAR51-07.

[20] M. Kassab, J. DeFranco and V. Graciano Neto, "*An Empirical Investigation on the*

Satisfaction Levels with the Requirements Engineering Practices: Agile vs. Waterfall," i IEEE International Professional Communication Conference (ProComm), Toronto, ON, Canada, 2018, ss. 118-124, doi: 10.1109/ProComm.2018.00033.

[21] M. A. Awad. 2005. A comparison between agile and traditional software development methodologies. *University of Western Australia*, 30, 1-69, doi: 10.1.1.464.609020190422-13963-j0ju8a

[22] W. Singhto, N. Denwattana, "*An experience in blending the traditional and Agile methodologies to assist in a small software development project*," i 13th International Joint Conference on Computer Science and Software Engineering (JCSSE), Khon Kaen, Thailand, 2016, ss. 1-5, doi: 10.1109/JCSSE.2016.7748914.

[23] S. Shirokova, E. Kislova, O. Rostova, A. Shmeleva, L. Tolstrup, "*Company efficiency improvement using agile methodologies for managing IT projects*," i Proceedings of the International Scientific Conference - Digital Transformation on Manufacturing, Infrastructure and Service (DTMIS '20). Association for Computing Machinery, New York, NY, USA, 2021, ss. 1-10, doi: 10.1145/3446434.3446465.

[24] P. Kurien, W. Rahman, V.S.Purushottam, "*The case for re-examining it effectiveness*" in Journal of Business Strategy. 2004. doi: doi/10.1108/02756660410525380. (Hämtad: 12 februari 2024).

[25] S. Schinagl, K. Schoon, R. Paans, "*A Framework for Designing a Security Operations Centre (SOC)*," i 48th Hawaii International Conference on System Sciences, Kauai, HI, USA, 2015, ss. 2253-2262, doi: 10.1109/HICSS.2015.270.

[26] A. Madani, S. Rezayi, H. Gharaee, "*Log management comprehensive architecture in Security Operation Center (SOC)*," i International Conference on Computational Aspects of Social Networks (CASoN), Salamanca, Spain, 2011, ss. 284-289, doi: 10.1109/CASON.2011.6085959.

[27] Z. Bakalova, M. Daneva, "*A comparative case study on clients participation in a 'traditional' and in an Agile software company*," i Proceedings of the 12th International Conference on Product Focused Software Development and Process Improvement (Profes '11). Association for Computing Machinery, New York, NY, USA, 2011, ss. 74-80, doi: 10.1145/2181101.2181118.

[28] S. Dushantha et al., *"SafeQR: An anti-phishing tool for automatically searching and parsing QR codes hidden in email attachments,"* c uppsats, Faculty of Social Sciences, University of Agder, Kristiansand, Norge, 2024. [Online]. Tillgänglig:

https://kompetansetorget.uia.no/content/download/182308/2789701/version/1/file/Report+IS-304+Final.pdf

[29] O. Lindström, *"Next Generation Security Operations Center,"* c uppsats, Information and Communications Technology, University of Applied Sciences, Finland, 2018. [Online]. Tillgänglig: https://www.theseus.fi/bitstream/handle/10024/157357/Lindstrom_Otto.pdf?sequence=1

[30] Mehmet Celepkolu and Kristy Elizabeth Boyer. 2018. Thematic Analysis of Students' Reflections on Pair Programming in CS1. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18). Association for Computing Machinery, New York, NY, USA, 771–776. https://doi.org/10.1145/3159450.3159516

[31] V. Braun, V. Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bilagor

Bilaga 1: Redovisning av sökförande

Söktermer inom IEEE

Sökord/Sökterm	Artikel	Sökträff
security operation center AND agile OR soc AND waterfall model	-	50
“security operation center” AND “challenge”	-	1,548
agil vs waterfall	-	0
agile vs traditional	[6], [20]	62
“security operations center” AND “SOC”	[25], [2]	663
“security operations center” AND “agile”	-	39
“security operations center” AND “waterfall”	-	6
“security operations center” AND “sequential”	-	105
"security operations center" AND ("Document Title":"method*")	-	15
security operations center AND small and medium-sized enterprises	-	21
waterfall to agile AND Security Operations Center	-	1
"waterfall or agile"	-	4
"waterfall to agile" AND Security Operations Center	-	0
waterfall to agile AND Small Medium Enterprise AND Security Operations Center	-	0
Agile AND Small Medium Enterprise AND Security Operations Center	-	0
Waterfall AND Small Medium Enterprise AND Security Operations Center	-	0
Small Medium Enterprise AND Security Operations Center	-	52
"waterfall to agile"	[11], [12]	11
waterfall to agile AND Small Medium Enterprise	[4]	3
“method*” AND "agile" OR "waterfall"	[5]	9,156
(“method*” AND "agile" OR "waterfall") AND (“small medium enterprise*” OR “small medium size*”)	[15]	126
“adaptability” AND “effective*” AND “agile”	-	27
"adapt*" AND “agile” AND “traditional”	[22]	246
"agile" AND "waterfall"	-	348
“security operation* center”	[8], [7]	224
“security operations center” AND “agile”	-	1
“security operations center” AND “waterfall”	-	0

Söktermer inom ACM

Sökord/Sökterm	Artikel	Sökträff
"security operations center" AND agile project management	-	45
"comparative study" AND "waterfall" AND "agile" AND "security operation center"	-	1
"comparative study" AND "waterfall" AND "agile"	[27]	60
"agile" AND "security operation center"	-	6
"Security Operations Center" AND "waterfall"	-	5
"security operation center" AND "challenge"	-	26
waterfall to agile AND security operations center AND small medium enterprise	[17]	128,103
"waterfall to agile" AND "small medium enterprise"	-	0
waterfall model AND small medium enterprise AND agile model	-	301,813
waterfall to agile AND "small medium enterprise"	-	12
agile efficiency and adaptability	[23]	303,849
(waterfall to agile) AND (efficiency and adaptability) AND ("small medium enterprise")	-	30241
agile AND efficiency AND ("small medium enterprise" OR "sme") AND adaptability AND security operation center	-	93
"security operations center" AND "agile"	-	13
"security operations center" AND "waterfall"	-	6

Söktermer inom Google Scholar

Sökord/Sökterm	Artikel	Sökträff
"comparative study" AND "waterfall"AND "agile" AND "security operations center"	-	4
"agile" AND "small medium enterprise" AND "security operations center"	-	0
"waterfall" AND "small medium enterprise" AND "security operations center"	-	0
"agile transformation" AND "security operations center"	-	6
"challenges in transitioning from waterfall to agile" AND "security operation center"	-	1
"small" AND "medium" AND "enterprise*" AND "agile method*"	[9]	2,760
"security operations center" AND "agile"	-	193
"waterfall to agile" AND "small medium enterprise"	-	2
"Small Medium Enterprise" AND "Security Operations Center"	-	4
case study agile and waterfall and small-medium enterprise	[19]	1 300
real case study agile and small-medium enterprise	[14]	11 700
agile methods in security operations center	-	173 000
"security operations center" AND "agile"	[28], [29]	672

“security operations center” AND “waterfall”	-	102
software traditional methods	[21]	omfattande

Kedjesökning/referenssökning

Ursprungsartikel	Snowballing Databas	Snowballing Artikel
[17]	ACM	[24]
[9]	Google Scholar	[10]
[2]	IEEE	[26]

Tabellen inkluderar en kedjesökning för att visa vilka artiklar som har refererat till andra forskningsmaterial. Tabellen visar ursprungsartikel (första kolumn), vilken databas som den kedjesöktna artikeln presenterar (kolumn två) och den relevanta artikeln inom den ursprungliga artikeln (kolumn tre). Det utfördes kedjesökning framåt, det vill säga artiklar som har använt andra artiklar. Detta utfördes på artiklar som har varit nära forskningsområdet av denna studie, med syfte att utöka mer relevanta artiklar för studien.

Bilaga 2: Omfattning av material

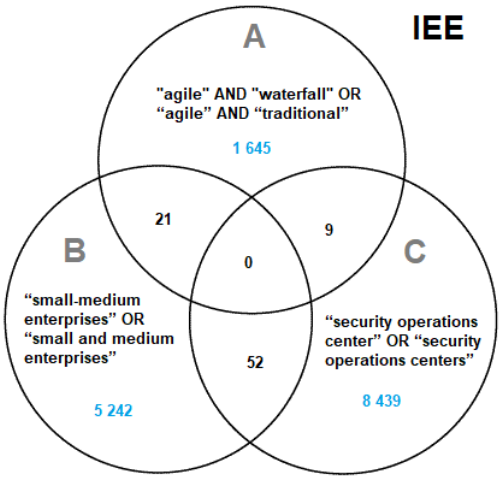
Första tabell:

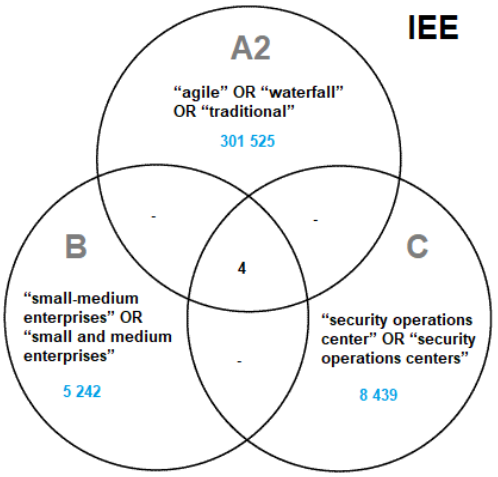
Fall	Sökterm	Sökträff		
		IEEE	ACM	Scholar
A	"agile" AND "waterfall" OR “agile” AND “traditional”	1 645	6 271	628 000
A2	“agile” OR “waterfall” OR “traditional”	301 525	229 726	4 730 000
B	“small-medium enterprises” OR “small and medium enterprises”	5 242	693	17 100
C	“security operations center” OR “security operations centers”	8 439	133	6 320

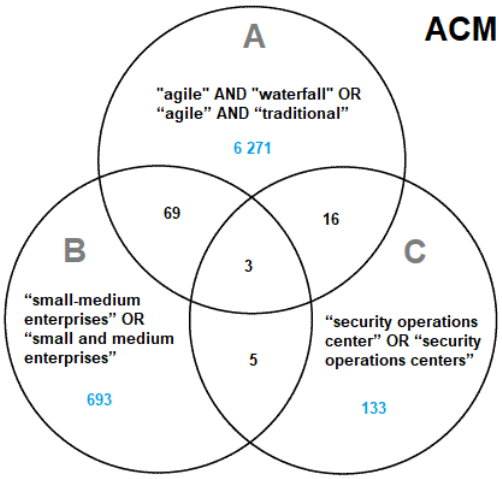
Andra tabell:

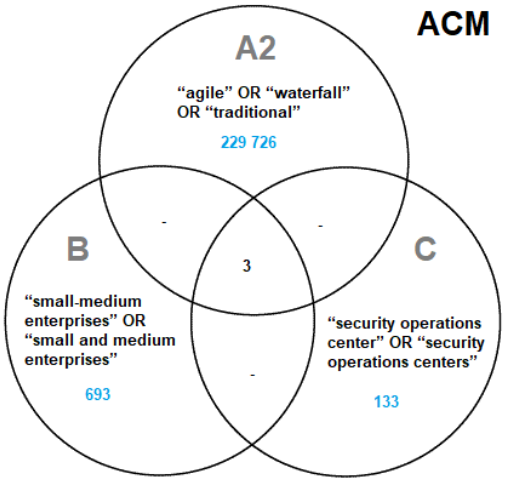
Fall	Sökträff		
	IEEE	ACM	Scholar
A & B	21	69	13 600
A & C	9	16	474
B & C	52	5	123
A & B & C	0	3	42
A2 & B & C	4	3	95

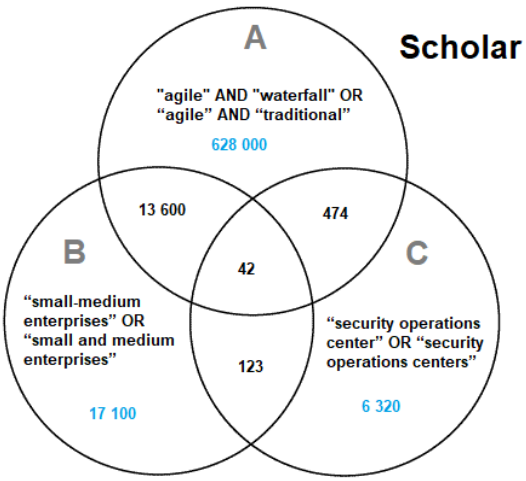
Venndiagram:

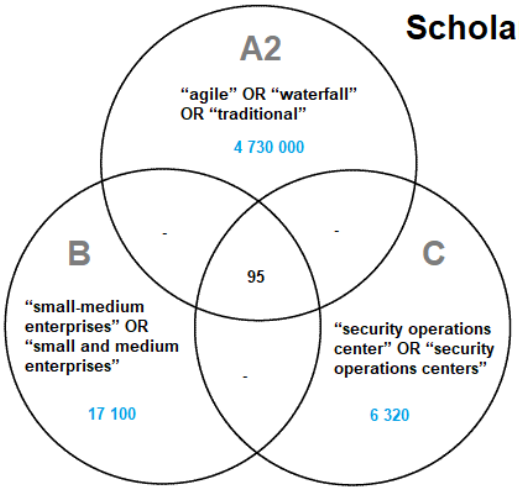












Bilaga 3: Kategorier av artiklar

Artikel	Publ. år/mån	Koncept				Typ av verksamhet
		Agil	Traditionell	SME	SOC	
[4]	2020 feb	*	*	*		Mjukvaruutvecklingsföretag
[11]	2008 aug	*	*			
[12]	2012 nov	*	*			
[6]	2021 nov	*	*			
[23]	2021 maj	*	*			
[9]	2021 okt	*	*	*		
[10]	2014 jun	*	*	*		
[20]	2018 sep	*	*			
[17]	2021 mar	*				
[15]	2018 dec	*	*	*		
[5]	2022 nov	*	*			
[22]	2016 nov	*	*			
[19]	2022 mar	*	*			
[14]	2010 feb	*		*		
[27]	2011 jun	*	*			
[7]	2020 dec				*	SOC och säkerhetstjänster
[8]	2018 aug				*	
[2]	2013 okt				*	
[25]	2015 mar				*	
[26]	2011 dec				*	
[28]	2024	*			*	Båda
[29]	2018 nov	*			*	

Matrisen visar samtliga artiklar med referensnummer, publiceringsmånad och år samt vilket koncept de tillhör. Vetenskapliga artiklar är kategoriserade efter koncepten agil, traditionell, SME och SOC. Dessa koncept är sedan uppdelade efter typ av verksamhet: mjukvaruutvecklingsföretag, SOC/säkerhetstjänster eller båda. Denna tabell har inspirerats från B. J. Oates [13, kap. 6].

Bilaga 4: Intervjufrågor

Nedan visas intervjufrågor till samtliga 6 intervjuer. Observera att även om huvudfrågorna behandlar hur SOC jobbar, är det en del av utmaningar som tas senare på generella frågor.

SVENSKA

Introduktionsfrågor

1. Kan du börja med att introducera dig själv och din erfarenhet relaterat till SOC?

Huvudfrågor (Planering, möte, dokumentation, samarbete)

2. Vilka är huvudsakliga uppgifter och ansvarsområden inom SOC?
    - Finns det olika huvudområden?
    - Vad finns det för regler och riktlinjer som påverkar arbetsprocessen?
3. Skulle du kunna beskriva arbetsprocessen från start till slut? T. ex. ett typiskt arbetsflöde.
    - Har alla samma arbetstider eller är det blandat?
    - Är arbetsprocessen samma för andra kollegor?
    - Finns det deadline för ett specifikt arbete som ska vara klart?
    - Hur ser möjligheten ut för kompetensutveckling?
    - Skulle du tänka dig att regelbundet utbilda personalen i teamet?
4. Hur planerar och fördelar ni arbete inom teamet?
    - Hur ofta ändras planeringen?
    - Kan du peka ut specifika utmaningar ni möter i denna planeringsprocessen och hur dessa påverkar ert arbete?
5. Hur ofta håller ni möten och hur organiserar ni dessa möten?
    - Vilken typ av möten är det?
    - Vilka deltar i dessa möten och vilka roller har de?
    - Hur utförligt är möten? Är möten strukturerade?
6. Kan du beskriva hur ni hanterar dokumentation inom SOC?
    - Vilka typer av information dokumenteras och under vilka faser?
    - När dokumenterar ni händelser?
7. Kan du beskriva hur ofta du samarbetar med andra kollegor?
    - Hur effektivt upplevde du detta?
    - Finns det något konflikt?
    - Hur kommunicerar ni med varandra?
    - Hur påverkar distansarbete ert samarbete och kommunikation?
    - Hur ofta anser du att det är möjligt att arbeta hemifrån?

Generella frågor (utmaning, förbättring)

8. Vilka utmaningar stöter du på i ditt nuvarande arbetssätt?
    - Inklusive verktyg, möten, dokumentation och planering.
9. Finns det specifika områden eller processer som kan förbättras?
    - Hur kan dessa förbättringar implementeras?

10. Vilka begränsningar ser du inom SOC-miljön särskilt med avseende på regler, riktlinjer och policies?
11. Vilka möjligheter ser du inom SOC-miljön särskilt med avseende på regler, riktlinjer och policies?

Avslutsningsfrågor

12. Har du någon tidigare erfarenhet av att arbeta med en agil arbetsmetodik? Om ja, kan du dela med dig av dina erfarenheter och hur du jämför den med det nuvarande arbetssättet?
13. Till sist, finns det något som du vill lägga till, som vi inte har tagit upp under intervjun? Det kan vara ytterligare insikter, erfarenheter, eller förslag relaterade till ditt arbete eller arbetsmetoder.

ENGLISH

Introductory questions

1. Could you start by introducing yourself and your experience related to SOC?

Main questions (Planning, meeting, documentation, collaboration)

2. What are the main tasks and areas of responsibility within the SOC?
    - Are there different majors?
    - What rules and guidelines are there that affect the work process?
3. Could you describe the work process from start to end? E.g. a typical workflow.
    - Does everyone have the same working hours or is it mixed?
    - Is the work process the same for other colleagues?
    - Is there a deadline for a specific work to be completed?
    - What does the opportunity for skill development look like?
    - Would you consider regularly training the staff in the team?
4. How do you plan and distribute work within the team?
    - How often does the planning change?
    - Can you point out specific challenges you face in this planning process and how these affect your work?
5. How often do you hold meetings and how do you organize these meetings?
    - What kind of meetings are they?
    - Who attends these meetings and what are their roles?
    - How detailed are meetings? Are meetings structured?
    - Retrospective
6. Can you describe how you handle documentation within SOC?
    - What types of information are documented and during which phases?
    - When do you document events?
7. Can you describe how often you collaborate with other colleagues?
    - How effective did you find this?
    - Is there a conflict?
    - How do you communicate with each other?

- How does remote work affect your collaboration and communication?
- How often do you consider it possible to work from home?

General questions (challenges, improvements)

8. What challenges do you encounter in your current way of working?
    - Including tools, meetings, documentation and planning.
9. Are there specific areas or processes that could be improved?
    - How can these improvements be implemented?
10. What limitations do you see within the SOC environment, especially with regard to rules, guidelines and policies?
11. What opportunities do you see within the SOC environment, especially with regard to rules, guidelines and policies?

Closing questions

12. Do you have any previous experience of working with an agile working methodology? If yes, can you share your experience and how it compares to the current way of working?
13. Finally, is there anything you'd like to add that we haven't covered below the interview? It may be additional insights, experiences, or suggestions related to your work or work methods.

Bilaga 5: Intervjuprotokoll

Datum	**Intervjuaren**	**Utrustning**
<datum>	Sossio Giorgelli, Habib Mohammadi	Inspelningsutrustning (om tillåtet). Ev. anteckningsmaterial (vid behov).

Tid, Plats	**Intervjuperson**
<tid>, <plats>	<intervjuperson>, <roll>

Presentation och Syfte

- Vi är två studenter (Sossio & Habib) som läser systemutvecklare på tredje året på Malmö universitet och vi gör vårt examensarbete hos [Organisationen] med fokus på traditionellt vs agil arbetsmetod.
- Syftet med vår examensarbete är att studera hur agil- eller traditionell arbetsmetod är lämplig för SOC (Security Operations Center).

- Syftet med den här intervjun är att studera nuvarande arbetsprocessen i [Organisationens] SOC avdelning, samt identifiera utmaningar som är relaterade till arbetsprocessen.

Användning och Bevarande av Data

- Intervjun kommer att bevaras anonymt, lagras säkert och användas enbart för examensarbetets syfte.

Bilaga 6: Mall för citat fördelning

Resp.	**<område, t.ex. dokumentation>**
1	<viktiga citat>
2	<viktiga citat>
3	<viktiga citat>
4	<viktiga citat>
5	<viktiga citat>
6	<viktiga citat>