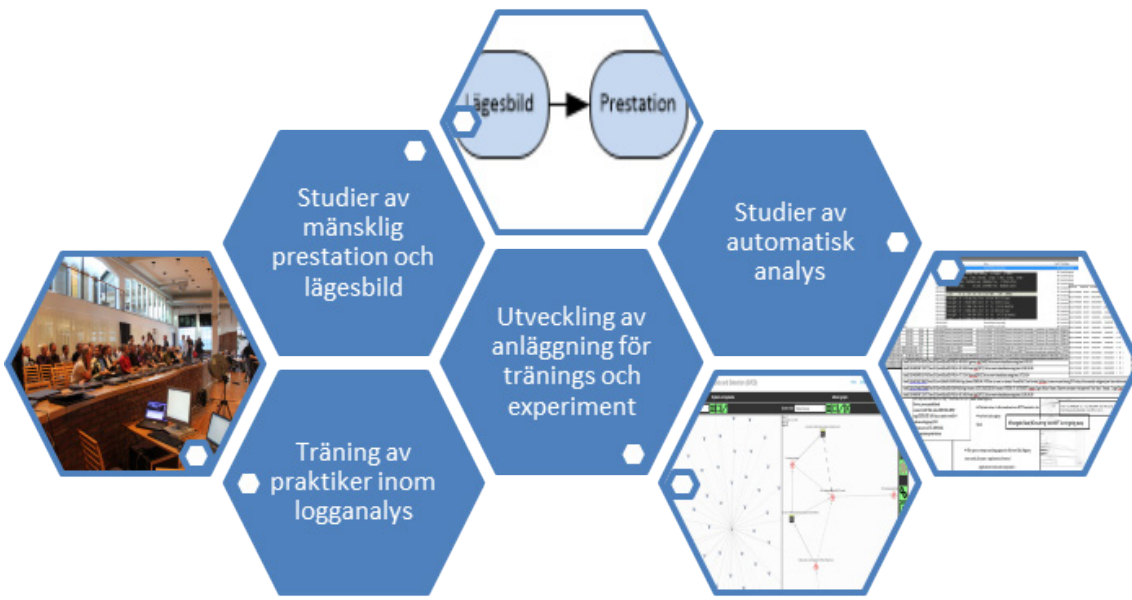
Övning och experiment för operativ förmåga i cybermiljön

Slutrapport

TEODOR SOMMESTAD



FOI-R--4498--SE
ISSN 1650-1942
December 2017

FOI-R--4498--SE

Teodor Sommestad

Övning och experiment för operativ förmåga i cybermiljön

Slutrapport

Titel	Övning och experiment för operativ förmåga i cybermiljön: Slutrapport
Title	Exercises and experiments for operational capability in the cyber environment: Final report
Rapportnr/Report no	FOI-R--4498--SE
Månad/Month	December
Utgivningsår/Year	2017
Antal sidor/Pages	28
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E72679
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

Ett cyberförsvar kräver flera olika förmågor. Det tre treåriga forskningsprojektet Övning och experiment för operativ förmåga i cybermiljön har inriktats mot den förmågan att analysera systemloggar för att upptäcka och förstå cyberangrepp. Projektet sökt svar på tre frågor. (1) Hur påverkas logganalysförmåga av olika faktorer? (2) Hur bör logganalysförmåga tränas och utvärderas? (3) Vilka verktyg krävs för experiment och övning av logganalysförmåga?

Svaret på den första frågan är att logganalysförmåga på en hög nivå är en funktion av förmågan till informationsinsamling, automatisk analys och manuell analys. Inom var och en av dessa finns flera variabler som har betydelse, men det finns begränsad kunskap om hur viktiga dessa är. Ett antal alternativa övningsupplägg togs fram som svar på den andra frågan och några försök gjordes med dessa. Det är tydligt att övning i kontrollerade cybermiljöer, där det rätta svaret är känt, är fördelaktigt. Svaret på den tredje frågan är att det krävs realistiska och meningsfulla cybermiljöer, verktyg för att simulera händelser i cybermiljön och verktyg som förenklar logginsamling. Projektet har arbetat med att FOI:s test- och övningsanläggning CRATE ska kunna tillgodose dessa behov.

Nyckelord: cyberförsvar, logganalys, intrångsdetektion, lägesbild, situationsmedvetande, träning, övning, prövning

Summary

A cyber defense requires several capabilities. The three-year project Exercises and experiments for operational capability in the cyber domain has focused on one the capability of analyzing system logs to detect and understand cyberattacks. The project has searched for answers to three questions. (1) How log analysis capability is influenced by different factors? (2) How should log analysis capability be assessed? (3) Which tools are required to run experiments and exercises on log analysis capability?

The answer to the first question is that log analysis capability is a function of the capability to collect information, automatic analysis, and manual analysis. Within these, a number of variables are of importance. However, the knowledge of how important they are is limited. A number of exercise alternatives were developed as an answer to the second question, and some of these were tested. It is apparent that exercises in controlled cyber environments, where the ground truth is known, is advantageous. The answer to the third question is that it requires realistic and meaningful cyber environments, tools to simulate events in the cyber environment, and tools that simplify log collection. The project has tried to ensure that FOI's cyber range CRATE can meet these requirements.

Keywords: cyber defence, log analysis, intrusion detection, situational awareness, training, exercise, assessment.

Innehållsförteckning

1 Inledning

Denna rapport sammanfattar det treåriga projektet Övning och Experiment för Operativ Förmåga i Cybermiljön (ÖvExCy). Detta första kapitel ger en kort bakgrund till projektet, beskriver dess inriktning och arbetspaket samt ger en läsanvisning till rapportens resterande delar.

1.1 Projektets frågeställningar

ÖvExCy startade 2015 inom ramen för Försvarsmaktens anslag för forskning och teknik (FoT). Projektet syftade till att utveckla kunskap om metod, organisation och teknik kopplat till operativ förmåga i cybermiljön. Kunskap om hur operativ förmåga både bör tränas och värderas skulle byggas upp. Dessutom skulle projektet, när så var lämpligt och möjligt, föreslå hur den operativa förmågan inom cybermiljön kan förbättras.

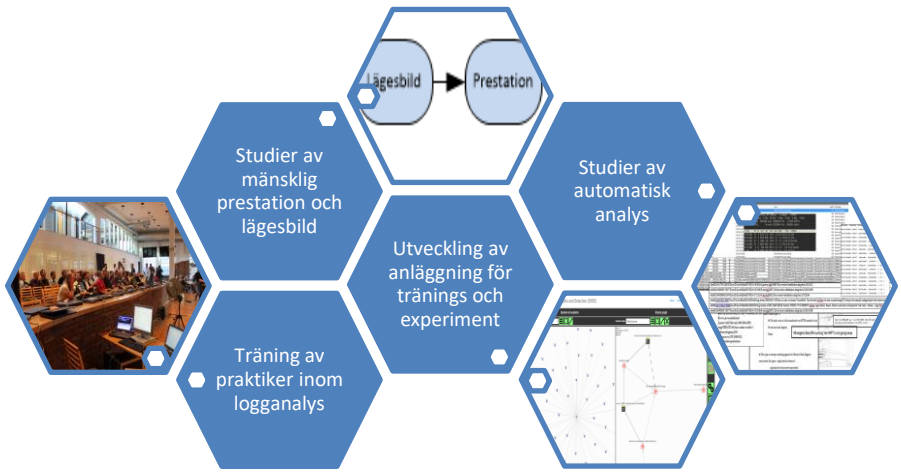
Operativ förmåga i cybermiljön kräver ett stort antal delförmågor. Alla dessa kan inte studeras i ett forskningsprojekt av ÖvExCy:s storlek (cirka två heltidsforskare per år). Efter diskussioner med Försvarsmakten bestämdes att projektet skulle fokusera på logganalysarbete, bland annat med anledning av att en ny logganalysenhet just skapats i Försvarsmakten. Projektets mål var att svara på följande frågor:

- **Hur påverkas logganalysförmåga av olika faktorer?**
  Eller mer precist, hur stödjer faktorer kopplade till metod, människa organisation och teknik dessa operativa förmågor inom cybermiljön?
- **Hur bör logganalysförmåga tränas och utvärderas?**
  Eller mer precist, vilka utbildningsscenarier och experiment är passande för att utveckla, pröva och utvärdera dessa operativa förmågor inom cybermiljön?
- **Vilka verktyg krävs för övning och experiment av logganalysförmåga?**
  Eller mer precist, hur bör en övnings- och experimentanläggning konstrueras för att effektivt stödja övning och experiment kopplade till dessa operativa förmågor inom cybermiljön?

Dessa tre frågor har adresserats parallellt under projektets gång.

1.2 Inriktning och arbetspaket

Fyra arbetspaket, illustrerade i Figur 1, har genomförts för att ge svar på de tre frågorna ovan. En stor del av arbetet har varit inriktat på att förbättra möjligheterna att träna Försvarsmaktens logganalytiker i den test- och övningsanläggning som finns på FOI. Det har i sin tur ställt krav på att kunna mäta lägesbild för att utvärdera prestation och lärande. Det har också krävt tekniska förbättringar av test- och övningsanläggning. Interaktionen med Försvarsmaktens logganalytiker har också gett projektet förståelse som varit till nytta i det fjärde arbetspaketet: tester av verktyg för automatisk analys.



Figur 1. De fyra arbetspaket i projektet Övning och Experiment för Operativ Förmåga i Cybermiljön.

Arbetet kopplat till träning och prestation har utförts i ett samarbete mellan forskare från kompetensområdet informationssäkerhet och kompetensområdet människa-system-interaktion. Inom arbetspaketen som utvecklat anläggningen och studerat verktyg för automatisk analys har ett visst samarbete skett med andra forskare inom FOI genom EU-projektet CORE. Därtill har projektet deltagit i NATO-gruppen IST-129 som är inriktad på att sammanställa kunskap om tekniker för att under pågående angrepp gissa angripares intentioner.

1.3 Läsanvisning

Denna rapport ämnar ge koncisa svar på de tre frågorna som beskrivits ovan. Svaren ges under rubriker som hör ihop med respektive fråga:

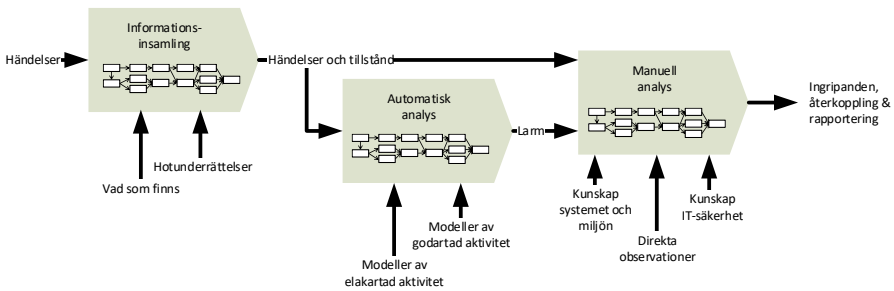
- Kapitel 2: Hur påverkas logganalysförmåga av olika faktorer?
- Kapitel 3: Hur bör logganalysförmåga tränas och utvärderas?
- Kapitel 4: Hur bör man träna och utvärdera logganalysförmåga?

Under varje rubrik ges först korta svar i form av en punktlista och därefter en förhållandevis kort beskrivning av bakgrunden till detta svar. Rapporten innehåller referenser till de rapporter, artiklar och memon som producerats i projektet och där resultaten beskrivs utförligare. Den intresserade finner en lista på dessa tillsammans med deras huvudsakliga bidrag i appendix.

2 Hur påverkas logganalysförmåga av olika faktorer?

- **Logganalysförmåga kan ses som en sammanslagning av förmågan till automatisk analys och manuell analys, och begränsas av hur väl informationsinsamlingen fungerar.**
- **Det finns många idéer om hur de olika förmågorna ska uppnås, särskilt när det kommer till automatisk analys. Dessvärre finns få ordentliga tester gjorda under realistiska förutsättningar och kunskapen om vilka tekniker och metoder som fungerar är därför bristfällig.**
- **Många automatiska analyser verkar lovande på pappret, men för i driftsatta system är den manuella analysen fortfarande av stor betydelse. Det finns goda förutsättningar att utveckla detta arbete med utgångspunkt från kunskap och tekniker som tagits fram forskning på mänskliga faktorer i relaterade discipliner.**

Under projektets första år ägnades en betydande andel av tiden till att gå igenom och sammanställa tidigare forskning inom logganalys för att identifiera de faktorer som påverkar logganalysförmåga. Resultatet av detta arbete är beskrivet i [1], där logganalysförmåga bryts ner i de tre delförmågorna informationsinsamling, automatisk analys och manuell analys (Figur 2). Dessa tre, och de delar de består av, är de faktorer som bestämmer den logganalysförmåga som uppnås.

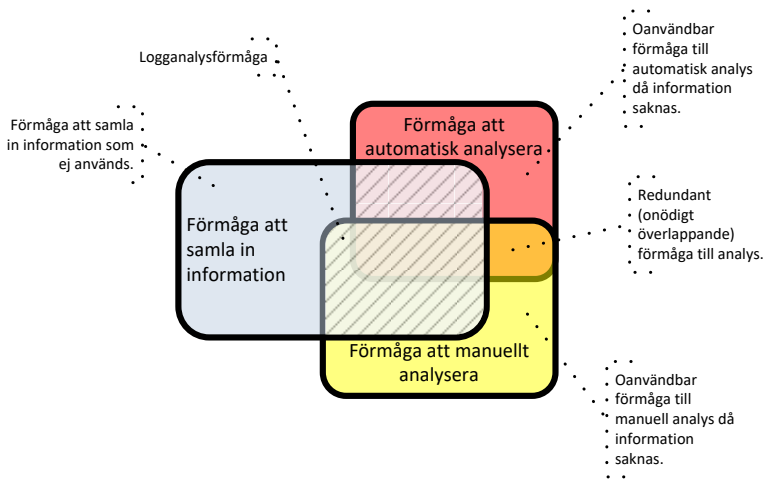


Figur 2. Översikt över logganalysarbete och den input och output som hanteras.

Det är naturligtvis svårt att utföra analyser av loggar utan att samla in dem. *Informationsinsamling* är därför en förutsättning för de andra två processerna, och förmågan att samla in händelser sätter en gräns för vilka analyser som kan utföras och hur bra resultatet kan bli. Analysen, i form av *automatisk analys* och *manuell analys*, bör komplettera varandra för att uppnå högsta förmåga. Det är också vanligt att logganalysarbete organiseras på ett sådant kompletterande sätt. I de flesta fall kompletterar automatiska analyser manuella analyser på så sätt att de ger en grov förbehandling av data som höjer informationskvaliteten, till exempel genom att markera vilka händelser (eller kombinationer av händelser) som troligast är kopplade till hot. Därefter tar vanligtvis den manuella analysen vid, och en människa undersöker de händelser som prioriterats med manuella eftersökningar. Givet att de tre delförmågorna informationsinsamling, automatisk analys och manuell analys skulle kunna mäta som någon sorts andel av alla totala förmågor det går att ha skulle följande formel kunna användas för att skatta logganalysförmåga:

Logganalysförmåga = Informationsinsamling ∩ (Manuell analys ∪ Automatisk analys)

Symbolerna ”∩” respektive ”∪” representerar här det matematiska snittet och unionen. Formeln utrycker bland annat att det inte går att uppnå maximal logganalysförmåga utan fullständig/perfekt informationsinsamling, att endast analysförmåga som kan utgå från tillgänglig information är till nytta och att automatiska och manuella analyser bör komplettera varandra snarare än överlappa varandra. Figur 3 tre illustrerar samma sak i ett venndiagram där det streckade området är den logganalysförmåga som resulterar av de tre delförmågorna.



Figur 3. Konceptuell visualisering av hur de tre förmågorna tillsammans skapar logganalysförmåga (streckat i figuren).

Det finns även en återkoppling från manuell analys till de andra två delförmågorna som inte visas i processdiagrammet i Figur 2. Resultatet av analyser kan nämligen också hjälpa till att identifiera vilken information som bör samlas in för att underlätta framtida arbete eller trimma in den automatiska analysen. Goda analyser kan alltså leda till bättre informationsinsamling. En något utförligare beskrivning av till de tre förmågorna ges nedan.

2.1 Informationsinsamling

Var och en av delförmågorna kan brytas ner i många enskilda faktorer som har mer eller mindre kända kopplingar till logganalysförmåga. Det finns god kunskap om vilken typ av *informationsinsamling* som behövs eftersom det följer direkt av de analyser som behöver utföras. Det finns också förhållandevis god kunskap om hur informationsinsamlingen bör göras. Till detta finns många olika typer av sensorer som kan användas för att hämta in händelser, och dessa har kända för- och nackdelar med avseende på exempelvis prestanda och hårdvarukrav. Det finns ett hanterligt antal mer eller mindre etablerade standarder för hur systemloggar ska se ut och sparas. Den forskning och utveckling som sker berör främst hanteringen av stora datamängder och insamling av hotunderrättelser som ska komplettera systemloggarna. Ett av problemen är att söka igenom enorma mängder halvstrukturerade loggposter. Ett annat är det ännu inte finns universella standarder för att dokumentera hotunderrättelser så att de blir lättanvända i framtida analyser eller för samarbetspartners.

2.2 Automatisk analys

Det finns en uppsjö av mer eller mindre färdiga förslag på hur *automatisk analys* ska genomföras. De automatiska analyserna kan grovt sägas bygga på antingen modeller av elakartad aktivitet, modeller av godartad aktivitet eller en kombination av dessa. Modeller av elakartad aktivitet fångar vanligtvis signaturer för kända angreppssteg eller tankar om hur angripare utför sekvenser angreppssteg; modeller av godartad aktivitet handlar typiskt om att använda statistiska modeller för att kunna larma ifall något avviker från det vanliga tillståndet i systemet.

Eftersom få ordentliga tester gjorts är de många lösningsförslagens träffsäkerhet i stort sett okänd. När kvantitativa tester av analysers träffsäkerhet görs används data som är gammal och saknar relevans för dagens logganalysproblem. Trots det bedömer många att det finns en stor potential inom automatisering, särskilt inom avancerade statistiska metoder som maskininlärning [2][3]. ÖvExCy hade planer på att testa ett stort antal föreslagna lösningar mot data skapad i CRATE, den test- och övningsanläggning som används i projektet. Dessa planer grusades dock

av svårigheten att få tillgång till färdiga lösningar. Av cirka 8000 vetenskapliga artiklar som publicerats inom intrångsdetektion mellan 2010 och 2015 identifierades femtio som både diskuterats bland forskare och som innehöll konkreta tester av en lösning som skulle kunna fungera i ett vanligt datornätverk. När FOI kontaktade författarna till dessa femtio artiklar och erbjöd sig att testa deras lösning var det endast tre som var beredda att göra sin implementation tillgänglig. Två av dessa bedömdes vara av begränsat värde för en logganalytiker i Försvarsmakten; den tredje lösningen, Snort Intrusion Analysis using Proof Strengthening (SnIPS) [4][5], testades inom projektet.

SnIPS, som pusslar ihop larm för att avgöra om en dator blivit komprometterad (d.v.s. övertagen) av en angripare, tycks erbjuda ett fullt fungerande sätt att öka kvaliteten på informationen som visas för en logganalytiker. Lösningen minskar antalet larmposter som behöver undersökas dramatiskt jämfört med ett grundfall där intrångsdetektionssystemet Snort används. Med ett tröskelvärde på 50 procent skulle en logganalytiker exempelvis kunna identifiera 25 procent av de komprometterade maskinerna genom att titta på 103 larmposter. Ifall 25 procent av de lyckade angreppen skulle behöva identifieras med slumpvis valda högprioritetslarm från Snort skulle över 2500 behöva undersökas (cirka 25 gånger fler än med SnIPS). Testet av SnIPS visade alltså på lovande resultat.

SnIPS, liksom många andra logganalyslösningar, bygger på intrångsdetektionssystemet Snort. Inom projektet har det även undersökts hur bra Snort är på att upptäcka angrepp av olika slag och i vilken utsträckning det klarar att identifiera nya (okända) angrepp [6]. Testet gjordes genom att slumpvis valda angreppskoder justerades så att de kunde utföras av i en generisk testmiljö som inte innehöll alla mjukvaror som var sårbara. Angreppskoderna skrevs bland annat om så att den utfördes även om maskinen i testmiljön inte var sårbar för angreppet och gav de svar som förväntades på frågor. Trafiken undersöktes av signaturdatabaser från flera olika år och utgivare. Mellan 8 och 25 procent av angreppen gav larm av rätt prioritet med de olika signaturdatabaserna och valet av signaturdatabas spelar alltså stor roll. Nyare signaturdatabaser var något bättre och publikt kända sårbarheter upptäcktes oftare. Det fanns även att inaktiverade signaturer kan tillföra värde. Med alla signaturer aktiverade upptäcktes drygt tre gånger så många angrepp.

Testen av Snort och SnIPS visar att det finns rimliga och fungerande automatiseringslösningar som förbättrar informationskvalitén. Det finns också enstaka tester av god kvalitet som undersökt andra förslag på automatisk analys. Andra tester av FOI har visat att det inte fungerar särskilt bra att filtrera Snorts larmposter baserat på information från sårbarhetsskanners [7] och en studie av larm producerade i en driftsatt universitetsmiljö har identifierat egenskaper i Snort-regler som reducerar antalet falsklarm [8]. Antalet föreslagna lösningar är dock stort medan testerna är få till antalet. De tester som finns är också i regel

avgränsade till särskilda förhållanden som är svåra att översätta till driftsatta system av den typ Försvarsmakten övervakar. Det saknas därför ordentligt empiriskt underlag för att avgöra vilka av alla föreslagna lösningar som är effektiva och värda att satsa på. Inte heller finns några väl belagda teorier om vilka ansatser som fungerar i driftsatta system. Till exempel fokuserar mycket forskning och marknadsföring i dagsläget på maskininlärning och ”artificiell intelligens”, men utan empiriska belägg för att det skulle fungera för att logganalys, där träningsdata oftast saknas och automatiska analyser bör vara transparenta för att stödja en efterföljande manuell analys.

2.3 Manuell analys

I driftsatta system används oftast enkla tekniker som larmar på enskilda händelser av misstänkt karaktär i de driftsatta systemen. Intrångsdetektionssystemet Snort, som utgår från en enkel signaturdatabas och undersöker nätverkstrafik, är ett exempel på en sådan enkel teknik. Att inte mer avancerade lösningar används, exempelvis sådana baserade på maskininlärning, beror sannolikt på att beläggen för de mer avancerade automationslösningarnas effektivitet är så bristfällig. Då systemen ofta producerar många larmposter om irrelevanta händelser och inte heller producerar särskilt mycket information om det misstänkta angreppet (t.ex. orsak eller allvarlighet) spelar den *manuella analysen* och logganalytikernas förmåga stor roll. I den manuella analysen bestämmer logganalytikerna hur insamling av information och automatisk analys ska genomföras; utför övervakning i den manuella analysen; analyserar händelsers orsak i den manuella analysen; samt väljer och utför åtgärder i den manuella analysen. Dessvärre finns också här få tillförlitliga studier om vilka variabler som är viktigast i dessa fall.

Medan antalet studier av logganalytiker och manuell analys ännu är få till antalet finns gott om kunskap från andra områden som kan ge en fingervisning av vad som är av betydelse för att människor ska prestera bra i en sådan analysroll. En genomgång av vilka mänskliga faktorer som kan tänkas påverka har gjorts i projektet [9]. På hög nivå ses logganalytikerns kognitiva förmåga (t.ex. korttidsminne), informationsresurser (t.ex. möjlighet att få återkoppling på analyser), kunskap om cybersäkerhet (t.ex. om olika angreppstyper) och arbetsplatsens utformning (t.ex. grafiska gränssnitt) vara de viktigaste faktorerna. Det finns även experimentella studier som antyder vilket stöd olika automatiska analyser ger till den manuella analysen. Exempelvis finns experiment som funnit att textbaserade gränssnitt ger mer detaljerade analyser och bra förmåga att se kända angrepp medan visuella gränssnitt gjorde det enklare att upptäcka nya typer av angrepp och anomalier [10]. Tyvärr finns också få studier som denna, och en stor andel av de som gjorts är gjorda mot testfall som saknar realism och/eller relevans för den logganalys som utförs i driftsatta system.

I projektet har FOI framförallt undersökt vilken information logganalytiker arbetar med och vilken information de bör nedteckna då de dokumenterar misstänkta incidenter eller meddelar varandra om misstänkta incidenter. Intervjuer med logganalytiker och litteraturstudier har utförts för att identifiera informationselement som anses lämpliga. Exempel på sådana är: information om tillgången som angripits, information om angriparen, mekanismer angriparen använt sig av och hur stor skada som skett. Två försök har utförts där alternativ testats med avseende på upplevd användbarhet och faktiskt användning [11][12]. Dessa pekar på att elementen som förs fram i praktiker-guider är rimliga och användbara. Oberoende bedömare tycks även ha lättare att begripa incidenterna ju fler informationselement som används.

3 Hur bör logganalysförmåga tränas och utvärderas?

- **Det är möjligt att använda simuleringsmiljöer för att både träna hela logganalysprocessen på ett holistiskt sätt och att träna uppgiftsfokuserat på en enskild del av den. Likaså finns goda skäl att träna enskilt som att träna i grupp.**
- **Avsaknaden av etablerade processer, tydlig praxis och väl definierade roller i området gör det svårt att hitta ett bra generellt svar på frågan. Processer, praxis och roller kan å andra sidan utvecklas med hjälp av träning, övning och prövning i simuleringsmiljöer.**
- **Simuleringsmiljöer ger goda möjligheter att ge tränade detaljerad återkoppling till sina analyser. Forskning på andra områden har visat att kvaliteten på återkoppling har en stor effekt på lärande och de försök som gjorts i projektet stödjer detta.**

Denna breda och svåra fråga har adresserats genom en genomgång av tänkbara alternativ för träning och övning samt utvalda ansatser till metodutveckling i samband med försök. Detta arbete beskrivs nedan.

3.1 Alternativ för träning och övning

I Försvarsmaktens Pedagogiska grunder [13] ges tio generella perspektiv på övning: mål med övningen, övningsdynamik, tid, sammanhang, förståelse, organisation, kunskapsaspekter, planering, frågor och läraren. Dessa, precis som mycket annat inom pedagogik, är relevanta för cybersäkerhetsövningar inom logganalys. Utifrån de uppgifter logganalytiker utför identifierades forskning på mänskliga faktorer kopplade till dessa uppgifter. Baserat på detta, samt etablerad kunskap inom pedagogikområdet, identifierades sju exempel på (cybersäkerhets)övningar som skulle kunna utföras. Tabell 1 sammanfattar dessa.

Tyvärr saknas i dagsläget instruktioner, manualer eller liknande som innehåller beskrivningar av hur logganalysuppgifter bäst utförs. Detta gör det svårt att lära ut arbetssätt genom att tydligt instruera deltagare i övningar, vilket är problematiskt och minskar möjligheten att lära ut effektiva arbetssätt. Samtidigt kan återkoppling som ges på prestationer vara träffsäker och direkt när det görs i samband med träning under kontrollerade former, vilket gör det möjligt att

använda träningen till att pröva sig fram till det bästa arbetssättet. Med anledning av detta bedömdes övningar av en explorativ karaktär med tydlig återkoppling vara av större värde i dagsläget.

Tabell 1. Sju exempel på övningar som skulle kunna utföras i en cyber range.

Uppgift	**Mänskliga faktorer**	**Pedagogisk poäng**
Manuell analys av loggar som inkluderar angrepp för att rekommendera åtgärder.	Kräver mycket egen informationssökning och innebär hög mental belastning.	Individuellt lärarande i en sammanhängande och komplex situation, likt den i vardagen.
Prioritera en stor mängd loggposter och rekommendera vilka som ska analyseras djupare.	Koncentrationsförmåga, korttidsminne och förmågan att snabbt genomsöka stora informationsmängder.	Att tillämpa tidigare erhållen kunskap eller heuristik på ett effektivt sätt.
Utföra en djupanalys av vilka resurser som påverkats av ett angrepp.	De mentala modeller och den förståelse analytikern har för angreppstypen kommer spela stor roll. Uppgiften saknar tidspress.	En realistisk momentövning där detaljerad återkoppling kan ges.
Utföra en djupanalys av vad som möjliggjorde ett angrepp och föreslå åtgärd.	De mentala modeller och den kunskap analytikern har om sårbarheter kommer spela stor roll.	En realistisk momentövning där detaljerad återkoppling kan ges.
Skapa en signatur som identifierar ett angrepp utifrån angreppsbeskrivning.	Uppgiften handlar om förståelse för sensorer och angrepp. Arbetsbelastning eller tidspress bör vara låg.	Svårigheten kan enkelt varieras och direkt feedback kan ges genom tekniska tester.
Procedurträning enligt en manual eller handbok om logganalysarbete.	Attityd och motivation är centralt för att deltagarna ska lyckas med uppgiften.	Instruktörer har möjlighet att förbereda sig för väl valda övningsscenarion.
Beredskapstest där arbetsbelastningen stegvis ökar och uppgiften blir mer intensiv.	Arbetsmiljön bör vara realistisk och deltagarna bör vara bekanta med den. Ett antal faktorer prövas, däribland motivation och anpassningsbarhet.	Ger insikter om egna begräsningar och förmåga att hantera stress snarare än ny faktakunskap. Bör endast ges till erfarna analytiker.

Projektet genomförde endast den första typen av övning i Tabell 1, manuell analys av loggar. Denna typ av övning gjordes både i form av moment där deltagare jobbade enskilt och i form av gruppuppgifter där flera jobbade med samma uppsättning loggar i olika roller. Både den individuella övning och gruppövning som genomfördes tillsammans med Försvarsmakten uppskattades av deltagarna som ansåg den vara lärorik, mycket verklighetstrogen och att den kommer vara till nytta i det dagliga arbetet. Det framkom även att deltagarna upplevde att de saknade en tydlig strategi för att lösa uppgiften, vilket återigen belyser behovet av väl definierade arbetsmetoder. Liknande slutsatser drogs från en gruppövning med tekniker från svenska kärnkraftverk.

3.2 Återkoppling och metodutveckling

Under de individuella övningarna med Försvarsmakten gjordes ett experiment för att undersöka om den detaljerade återkopplingen var av betydelse. Under övningen producerades incidentrapporter nedskrivna enligt förbestämda fält som syftade till att mäta situationsmedvetenhet vid en viss tidpunkt. Återkopplingen gavs i form av det korrekta svaret verkade ha en positiv effekt. Deltagarna ansåg att det lärt sig mer efter att de fått det korrekta svaret än innan de fått det. De hade också en något mer positiv utveckling av sin prestation än en kontrollgrupp som inte fick återkoppling alls.

Det är värt att notera att kontrollerade övningar i princip är en förutsättning för att kunna ge god återkoppling till logganalytiker. Detta eftersom det saknas full kunskap om angrepp i det vardagliga arbetet där angriparna gör sitt bästa för att dölja sina aktioner. Därtill ställer kontrollerade övningar med tydliga mål krav på att utreda eller bestämma vad som ska övas och vad en bra prestation är. De kräver alltså att steg tas mot etablerade processer, tydlig praxis och väl definierade roller.

Efter försök med mallen för incidentrapporter föreslog också logganalytikerna från Försvarsmakten justeringar och förbättringar som syftade till att göra den mer användbar i deras verksamhet. Träningen bidrog därmed även till att skapa kunskap om vad logganalysarbete innebär och att definiera logganalysuppgiften. Efterföljande test av en vidareutveckling av denna mall gav ytterligare stöd för att de informationselement som togs fram var relevanta och hade värde i en incidenthanteringsprocess.

4 Vilka verktyg krävs för experiment och övning av logganalysförmåga?

- **Lösningar som gör träningsmiljöer mer tillgängliga är önskvärda. Dessa lösningar kan till exempel vara bibliotek över analysuppgifter som deltagare kan starta när det finns tid över.**
- **Tester visar att enklare atomära angrepp sannolikt är irrelevanta för en aktör som Försvarsmakten och att fokus bör ligga på att simulera mer komplexa angrepp som innehåller flera steg.**
- **Projektet har tagit fram SVED, ett verktyg som gör det möjligt att bygga bibliotek över komplexa angreppssekvenser som kan utföras på begäran eller vid bestämda tidpunkter.**

Tillsammans med tidigare projekt kopplat till övning och träning inom cybersäkerhet har ÖvExCy gett goda insikter i de behov och önskemål som praktiker har när det kommer till övningar. Genom åren har FOI har också samlat på sig ordentligt med erfarenhet från tekniska tester inom cybersäkerhet och logganalys. Många av kraven relaterade till övning, träning och test av logganalysförmåga överlappar helt eller delvis. De flesta tillämpningar kräver nämligen verktyg för att hantera

1) realistiska cybermiljöer
2) händelser i cybermiljön
3) sensorer och logganalysverktyg.

Då det finns ett allmänt behov av att minska de resurser som krävs för att skapa en övning eller ett träningstillfälle har mycket av arbetet handlat om att förbereda miljön för att öva logganalytiker. Hur det arbetet utförts beskrivs nedan i relation till de tre verktygstyperna.

4.1 Realistiska cybermiljöer

När det kommer till att konstruera realistiska cybermiljöer har cybermiljöer som liknar Försvarsmaktens egna skapats i CRATE med hjälp av de grundläggande verktyg som redan fanns att tillgå. Dessa cybermiljöer är snarlika

Försvarsmaktens på en hög nivå men är på intet sätt identiska med faktiska miljöer. Till exempel är det affärssystem som finns i de miljöerna betydligt enklare än det affärssystem som Försvarsmakten använder (dvs. PRIO). Inte heller används samma versioner av mjukvaror (t.ex. Microsoft Word), samma konfigurationer för nätverksutrustning (t.ex. brandväggar) eller samma användarinformation (t.ex. lösenord). När det kommer till realistiska cybermiljöer finns alltså förbättringspotential. Det finns samtidigt uppenbara problem kopplade till sådana förbättringar. Att återskapa komplexa system (exempelvis affärssystem) är kostsamt och kan kräva att ytterligare licenskostnader betalas. Dessutom kräver återskapande av detaljer i systemen att anläggningen och miljöbeskrivningarna skyddas – det skulle nämligen kunna ge information om eventuella säkerhetsbrister i Försvarsmaktens system. Vissa delar är också problematiska att samla in eller replikera fullt ut. Till exempel lagras vanligtvis inte lösenord i IT-system utan endast resultatet av att en kryptografisk envägsfunktion applicerats på lösenordet (en så kallad ”lösenordshash”). För att kunna simulera användare med deras riktiga lösenord krävs därför att användarna uppger lösenorden när cybermiljön skapas. Under projektet har dock inte realismen i cybermiljöerna upplevts som en begränsande faktor då det finns mycket av relevans som kan övas och testas i generella miljöer.

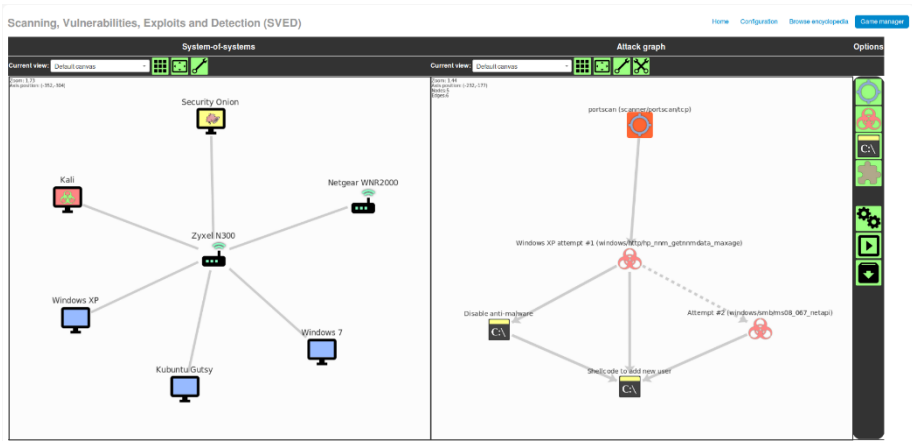
4.2 Händelser i cybermiljön

Projektet har gjort betydande framsteg när det kommer till hantering av händelser i cybermiljön. Det mesta av detta arbete är knutet till mjukvaran *Scanning, Vulnerabilities, Exploits And Detection* (SVED). Detta verktyg möjliggör planering och orkestrering av olika händelser som ska ske i den cybermiljö som skapats. Utifrån tester konstaterades att ogenomtänkta och enkla angrepp sällan lyckas mot driftsatta mjukvaror även om deras specifikationer indikerar att de skulle göra det. I ett av de större testen sårbarhetsskannades 725 datorer för att identifiera sårbarheter som det fanns passande publikt tillgängliga attackkoder för enligt skannerverktyget. Av 1545 angreppsförsök med grundinställningar lyckades bara 70 (4,5%); av 211 använda attackkoder fungerade endast 18 (8,5%) vid något försök. Även om verktyg som kan utföra atomära angrepp utifrån enkla beslutsmodeller är enkla att konstruera och simulera utgör de alltså ett begränsat hot och motsvarar inte den hotbild Försvarsmakten möter.

Verktyget SVED är byggt för att kunna hantera och dokumentera komplexa angrepp som sker i flera steg. SVED kan användas för att specificera angrepp en sekvens av angreppsförsök där viss fördröjning ska finnas mellan stegen och utfallet av angreppsförsöket påverkar vilka framtida steg som tas. Figur 4 visar en enkel sekvens av detta slag. I denna sekvens anger den streckade pilen att angreppssteget i slutet av pilen ska utföras om det tidigare angreppssteget misslyckats. De heldragna pilarna anger att dessa alltid ska utföras givet att

aktionerna innan utförts. SVED kan på samma sätt användas för att beskriva hur olika datoranvändare ska bete sig (t.ex. webbsidor som ska besökas) och instruera mjukvaran i cybermiljön utföra detta beteende på fördefinierade tidpunkter. Därtill är SVED integrerat med systemet som hanterar cybermiljöerna och kan till exempel återställa miljön till ett tidigare tillstånd före eller efter en händelsesekvens.

Då SVED orkestrerar alla dessa händelser ger det också en mycket detaljerad dokumentation av vilka händelser som utfördes vid olika tidpunkter. Till exempel går det att följa upp vilken millisekund ett angrepp utfördes mot en hemsida, vilken millisekund angriparen fick kontroll över datorn som kör hemsidan, när skadlig kod planterades på hemsidan och vilken sekund vanliga datoranvändare besökte samma hemsida. Förutom ett enkelt grafisk gränssnitt erbjuder SVED ett välutvecklat programmatiskt gränssnitt (API) som gör det möjligt att snabbt skapa komplexa händelsesekvenser enligt något mönster. Till exempel kan händelser enkelt kopieras mellan cybermiljöer som liknar varandra (t.ex. om flera övningsdeltagare ska angripas på samma sätt) eller om sekvensen ska varieras på ett genomtänkt sätt under ett experiment.



Figur 4. Planeringsvy i SVED:s webb-GUI. Till vänster syns ett enkelt datornätverk I cybermiljön; till höger syns en enkel attacksekvens mot datorer i datornätverket.

SVED:s funktioner innebär betydande fördelar mot manuella tekniker vid planering, genomförande av tester och betydande fördelar vid uppföljning av övning och träning. Det finns många idéer på hur SVED kan utökas för att ytterligare förenkla arbetet runtomkring övningar, träning och test. Till exempel finns idéer på hur databaser med incidentrapporter skulle kunna tolkas för att producera realistiska attacksekvenser och hur artificiell intelligens skulle kunna användas för att utföra realistiska automatiserade tester av datornätverk.

Ytterligare beskrivningar av SVED och dess funktioner finns i tidigare publicerade rapporter [14] [15].

När det kommer till simulering av godartad användaraktivitet har det gjorts tester av hur bildigenkänning skulle kunna användas för att styra datorer utan att göra avtryck i cybermiljön [16]. Detta tycks inte vara en väg framåt i dagsläget.

4.3 Sensorer och logganalysverktyg

Två förbättringar har gjorts kopplat till hantering av sensorer och logganalysverktyg. Inför övningar och experiment med fokus på logganalys är det naturligtvis viktigt att loggar finns att tillgå. Vilka verktyg för automatisk analys som önskas skiljer sig typiskt mellan olika övningar och experiment, men händelser (t.ex. datapaket i nätverket) är desamma. Avsaknaden av ett enkelt sätt att administrera logginsamling ledde till vissa bekymmer i samband med övningar, bland annat då de övade som skulle konfigurera den automatiska analysen saknade den kunskap om CRATE som krävdes för att sätta upp en bra logginsamling. Projektet har projektet skapat ett enkelt system där en lista på loggproducerande system anges tillsammans med önskad lagringsplats. Filerna kopieras sedan med hjälp av Virtualbox API så att de är enkelt åtkomliga på lagringsplatsen. Även om denna enkla lösning har begränsningar i prestanda, och inte kan hantera stora datamängder, bedöms det tillräckligt för de flesta övningar och experiment.

Därutöver har ett stödsystem för att koordinera övningar prövats i projektet. Detta system kallas *CRATE Exercise Control* (CEC) och hanterar schemaläggning av inspel, kommunikation mellan deltagare, till sammanställning av övningens progress och återkoppling till deltagarna. CEC har utvärderats i samband med en incidenthanteringsövning med deltagare från IT-avdelningar på svenska kärnkraftverk. Verktyget gav en tydlig förbättring mot det virrvarr av verktyg (kalkylark, chattprogram etc.) som använts i tidigare övningar. Ett antal tänkbara förbättringar identifierades. Däribland en tätare integration med SVED och särskilda funktioner för att i realtid särskilja observatörers rapporter från andras rapporter.

5 Förslag på framtida forskning

Det är tydligt att det med hjälp av en *cyber range* går att utföra ett stort antal tester som ger information om tekniska produkter och mänskliga förmågor. Värdet av dessa tester begränsas i huvudsak av den realism som kan åstadkommas i cybermiljön, händelserna och logganalysverktygen. Delar av denna realism kan uppnås genom rena utvecklingsinsatser. Till exempel behöver cybermiljöerna bli ännu mer realistiska för att kunna användas i prövande övningar eller skarp träning. Detta kan uppnås genom att de mjukvaror som används i cybermiljöerna införskaffas och konfigureras på rätt sätt. Andra saker kräver forskning och kunskapsutveckling. Framförallt behövs forskning för att kunna automatgenerera godartade och elakartade händelser som är realistiska i en försvarsmaktsmiljö. Att simulera ett förbestämt beteende med några utvalda applikationer är trivialt; att simulera komplexa beteenden som involverar interaktion och en stor mängd olika applikationer är svårt. Att simulera en angripare som är en okunnig nybörjare är trivialt; detsamma kan inte sägas om att simulera en kompetent angripare man vet lite om. Det behövs alltså kunskap om hur realistiska händelsemönster ser ut och verktyg för att generera dessa i en övningsmiljö eller testmiljö.

Cybermiljön, händelserna och logganalysverktygen syftar till att möjliggöra effektiva tester och övningar. De tester som gjorts hittills har trots sin enkelhet varit av påtagligt värde och fler tester av logganalysverktyg och arbetsmetoder för logganalysarbete bör utföras. I allmänhet finns ett behov av att etablera praxis och procedurer, då domänen i många avseenden saknar väldefinierade roller och förmågekrav. Sådant utvecklas och testas rimligen med fördel i en kontrollerad miljö. Ett konkret exempel på en praxis som kan etableras genom övning och prövning i en cyber range är standarder för utbyte av hotunderrättelser, vilket ÖvExCy varit inne på. Men det bör även göras undersökningar av vilken kunskap och vilka grundläggande förmågor och attityder som gör att en person är eller blir en bra logganalytiker.

6 Referenser

[1] T. Sommestad och H. Holm, “Variabler av vikt för förmågan att analysera cybersäkerhetsloggar (FOI-R--4126--SE),” Linköping, Sweden, 2015.

[2] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, och W.-Y. Lin, “Intrusion detection by machine learning: A review,” *Expert Syst. Appl.*, vol. 36, no. 10, pp. 11994–12000, Dec. 2009.

[3] J. M. Estevez-Tapiador, P. Garcia-Teodoro, och J. E. Diaz-Verdejo, “Anomaly detection methods in wired networks: A survey and taxonomy,” *Comput. Commun.*, vol. 27, no. 16, pp. 1569–1584, 2004.

[4] X. Ou, S. R. Rajagopalan, och S. Sakthivelmurugan, “An empirical approach to modeling uncertainty i intrusion analysis,” in *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 2009, pp. 494–503.

[5] S. C. Sundaramurthy, L. Zomlot, och X. Ou, “Practical IDS alert correlation in the face of dynamic threats,” i *The 2011 International Conference on Security and Management*, 2011.

[6] T. Sommestad och H. Holm, “Publika attackkoder och intrångssignaturer: Kvantitativa tester av träffsäkerhet (FOI-R--4499—SE),” Linköping, Sweden, 2017.

[7] T. Sommestad och U. Franke, “A test of intrusion alert filtering based on network information,” *Secur. Commun. Networks*, vol. 8, no. 3, pp. 2291–2301, Sep. 2015.

[8] E. Raftopoulos och X. Dimitropoulos, “A quality metric for IDS signatures: in the wild the size matters,” *EURASIP J. Inf. Secur.*, vol. 2013, no. 1, p. 7, 2013.

[9] P. Lif och T. Sommestad, “Human factors related to the performance of intrusion detection operators,” i *Human Aspects of Information Security, Privacy, and Trust*, 2015.

[10] R. S. Thompson, E. M. Rantanen, W. Yurcik, och B. P. Bailey, “Command line or pretty lines?: comparing textual and visual interfaces for intrusion detection,” i *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2007, p. 1205.

[11] P. Lif, H. Holm, T. Sommestad, M. Granåsen, och E. Westring, “Genomförd försöksverksamhet inom logganalys för cybersäkerhet,” Linköping, Sweden, 2016.

[12] P. Lif, T. Sommestad, och D. Granåsen, “Informationselement i incidentbeskrivningar: Framtagning och utvärdering under övningen iPILOT (FOI-R--4501--SE),” Linköping, Sweden, 2017.

[13] Försvarsmakten, *Pedagogiska grunder*. Stockholm: AerotechTelub Information & Media AB, 2006.

[14] H. Holm och T. Sommestad, “SVED: Scanning, Vulnerabilities, Exploits and Detection,” i *MILCOM 2016*, 2016.

[15] H. Holm och T. Sommestad, “So long, and thanks for only using readily available scripts,” *Inf. Comput. Secur.*, vol. 25, no. 1, pp. 47–61, Mar. 2017.

[16] M. Estgren, “Lightweight User Agents,” Linköpings universitet, 2016.

Appendix

Publikation	Huvudsakligt bidrag
P. Lif, M. Thorstensson, T. Sommestad, “Övning, träning och prövning inom logganalys - Översikt över olika alternativ,” FOI-R--4149—SE, 2015	Beskrivning av hur träning inom logganalys bör genomföras baserat på teorier och erfarenhet kring träning i cybersäkerhetsdomänen och i andra domäner.
P. Lif och T. Sommestad, “Human factors related to the performance of intrusion detection operators,” in *Human Aspects of Information Security, Privacy, and Trust*, 2015.	Sammanställning av vilka mänskliga faktorer som kan tänkas påverka logganalytikers prestation och de tester som finns att tillgå för dessa förmågor.
T. Sommestad, H. Holm, “Variabler av vikt för förmågan att analysera cybersäkerhetsloggar,” FOI-R--4126--SE, 2015	En beskrivning av de faktorer som påverkar logganalysförmåga och vad forskningsläget säger om deras relativa vikt för att uppnå logganalysförmåga.
T. Sommestad, ”Utveckling av CRATE inom ÖvExCy”, FOI Memo 5502, 2015.	Översiktlig beskrivning av de tekniska verktyg som har skapats, och som ska skapas, för att underlätta övning och träning av logganalytiker i CRATE.
T. Sommestad, “Experimentation on operational cyber security in CRATE”, NATO STO-MP-IST-133 Specialist Meeting, 2015’	Sammanfattning av den forskning som utförts med hjälp av CRATE i tidigare projekt och resonemang kring behovet av kvantitativa tester i cybersäkerhetdomänen.
P. Lif, H. Holm, T. Sommestad, M. Granåsen, E. Westring, “Genomförd försöksverksamhet inom logganalys för cybersäkerhet”, FOI-R--4328--SE, 2016.	Sammanfattning av den kontrollerade övning som utfördes under 2016 tillsammans med resultat kopplade till lärandeeffekt och användning av informationselement.
H. Holm, T. Sommestad, “SVED: Scanning, Vulnerabilities, Exploits and Detection,” MILCOM 2016, 2016.	Teknisk beskrivning av händelsehanteringsverktyget SVED för en internationell publik.
H. Holm. ”Teknikutveckling under 2016 inom Övning och Experiment för Operativ Förmåga i Cybermiljön”, FOI Memo 5856, 2016.	Sammanfattning av vidareutvecklingen av SVED och det användningstest som utfördes i samband med en övning.

Publikation	Huvudsakligt bidrag
T. Sommestad, H. Holm, “Test av logganalysverktyget SnIPS,” FOI-R--4323--SE, 2016.	Beskrivning av det test som utförts av loggkorrelationsverktyget verktyget SnIPS.
M. Estgren, “Lightweight User Agents,” Linköpings universitet, 2016.	Undersökt bildigenkänningsverktygs träffsäkerhet när de tillämpas på datorskärmar av olika slag och typ.
T. Sommestad, H. Holm, “Alert verification through alert correlation—An empirical test of SnIPS,” Information Security Journal: A Global Perspective, vol. 26, no. 1, pp. 39–48, Jan. 2017.	Beskrivning av det test som utförts av loggkorrelationsverktyget verktyget SnIPS för en internationell publik.
P. Lif, M. Granåsen, T. Sommestad, “Development and validation of technique to measure cyber situation awareness,” International Conference on Cyber Situational Awareness, Data Analytics and Assessment, 2017.	Presentation av ett förslag på informationselement som bör användas för beskrivning av cybersäkerhetsincidenter och det test som utförts av deras relevans.
H. Holm, T. Sommestad, “So long, and thanks for only using readily available scripts,” Information and Computer Security, vol. 25, no. 1, pp. 47–61, Mar. 2017.	Test av attackkoders tillförlitlighet utfört med verktyget SVED. Resultatet visar att de flesta attackkoder inte fungerar under förutsättningar som antyder att de borde.
T. Sommestad, H. Holm, ” Publika attackkoder och intrångssignaturer: Kvantitativa tester av träffsäkerhet”, FOI-R--4499—SE, 2017.	Test av attackkoders tillförlitlighet och test av publika signaturdatabasers förmåga att upptäcka publika angrepp.
T. Sommestad, H. Holm, Utveckling av CRATE inom ÖvExCy under 2017, FOI Memo 6258, 2017.	Beskrivning av förbättringar av verktyget SVED, utveckling av logginsamlingsstöd i CRATE och test av verktyg för övningsplanering och övningshantering.
P. Lif, T. Sommestad, D. Granåsen, ” Informationselement i incidentbeskrivningar: Framtagning och utvärdering under övningen iPILOT”, FOI-R--4501—SE, 2017.	Undersökning av hur olika informationselement bör användas för att dokumentera och sprida lägesinformation kopplade till angrepp samt test av hur de uppfattas av praktiker i en incidenthanteringsövning.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se