Informationselement i incidentbeskrivningar

Framtagning och utvärdering under övningen iPILOT

PATRIK LIF, TEODOR SOMMESTAD, DENNIS GRANÅSEN

FOI-R--4501--SE
ISSN 1650-1942 December 2017

FOI-R--4501--SE

Patrik Lif, Teodor Sommestad, Dennis Granåsen

Informationselement i incidentbeskrivningar

Framtagning och utvärdering under övningen iPILOT

Titel	Informationselement i incidentbeskrivningar
Title	Information elements in incident descriptions
Rapportnr/Report no	FOI-R--4501--SE
Månad/Month	December
Utgivningsår/Year	2017
Antal sidor/Pages	34
ISSN	1650-1942
Kund/Customer	FM
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

Vid cybersäkerhetsincidenter är en av de viktigaste uppgifterna att dokumentera det inträffade för att i efterhand kunna spåra vad som har hänt. Flera ramverk har utvecklats för att stödja dokumentationsarbetet, alla med sina för- och nackdelar. Som ett första steg i att utveckla en praktiskt användbar incidentbeskrivningsstandard har spårbarhets- och analysbehovet studerats för att identifiera vilken information som är lämplig att rapportera.

I denna rapport presenteras ett konkret förslag på 16 informationselement (t.ex. rapportör, angriparens nod och syfte bakom attacken) att inkludera i en incidentbeskrivning. Under en nationell cybersäkerhetsövning utvärderades förslaget avseende: (1) i vilken omfattning föreslagna informationselement nyttjades, (2) om elementen samvarierade med incidentbeskrivningarnas kvalitet och (3) deltagarnas subjektiva upplevelser av att använda elementen. Resultaten visar att vilka informationselement som användes varierar mycket, vilket var förväntat eftersom det t.ex. är betydligt enklare att beskriva vad som observerats och vilken nod som attackerats än att beskriva angriparen. Analysen visade också att incidentbeskrivningar med fler ifyllda informationselement generellt bedömdes ha högre kvalitet. Det fanns en tydlig träningseffekt från dag ett till dag två där poängsättningen ökade markant per inlämnad rapport.

Även om den övergripande bedömningen av den framtagna förenklade incidentbeskrivningen är positiv så indikerar deltagarnas subjektiva skattning av om rätt informationselement inkluderades under övningen att frågan bör utredas vidare.

Nyckelord: cybersäkerhet, logganalytiker, logganalys, informationselement, incidentbeskrivning.

Summary

In cybersecurity incidents one of the most important tasks is to report what has occurred. Several frameworks have been developed to support documentation work, all with their pros and cons. As a first step in developing a practically useful incident description standard, traceability and analysis needs have been studied to identify what information is appropriate to report.
This report presents a concrete proposal with 16 information elements to include in an incident description. The proposal was then evaluated during an exercise with 30 participants regarding the extent to which suggested information elements were used, if the elements matched the quality of the incident descriptions and the participants' subjective experiences of using the elements. The results show that the use of information elements varies a lot, which was expected because it is much easier to describe what was observed and what node was attacked than to describe the attacker. The analysis also showed that the completion of the information elements correlated with the quality of the incident descriptions, i.e. the incident descriptions with more completed elements were judged to be of higher quality. Also, there was a training effect from day one to day two, where the score increased significantly per submitted report.

Although the overall assessment of the simplified incidence description was positive, participants' subjective estimation of whether the right information elements were included in the incident descriptions during the exercise suggests that the question should be further investigated.

Keywords: cyber security, log analyst, log analysis, information element, incident description.

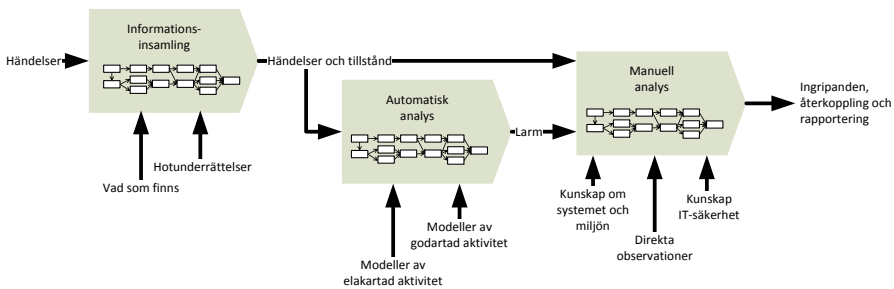
Innehållsförteckning

1 Inledning

Denna rapport är framtagen som en del av projektet Övning och experiment för operativ förmåga i cybermiljön (ÖvExCy). Projektet har bland annat undersökt hur incidenter bör beskrivas och kommuniceras för att logganalytiker ska kunna upprätthålla bra situationsmedvetande. Rapporten beskriver en utvärdering för att undersöka vilka informationselement som är lämpliga att dokumentera i logganalysarbete vid incidentbeskrivning. Ett antal tester genomfördes i samband med en övning i oktober 2017. Detta inledande kapitel ger en kort översikt över logganalysarbete i allmänhet, den del av logganalysarbete som handlar om incidentbeskrivningar och rapportens struktur.

1.1 Logganalysarbete

Cybersäkerhet saknar en tydlig och enhetlig definition men det finns flera övergripande idéer om vad begreppet innefattar och vilket arbete det kräver. Till exempel beskriver ramverket NICE från amerikanska National Institute for Standards and Technology (NIST) att det finns 928 uppgifter, 359 kompetenser och 614 kunskapsaspekter kopplade till yrkesroller inom cybersäkerhet (Newhouse, Keith, Scribner, & Witte, 2017). Denna rapport fokuserar på det som i NICE betecknas som *Computer Network Defence Analysis* och den yrkesroll som kallas logganalytiker. Logganalytikerns huvudsakliga uppgifter är att övervaka, analysera och fatta besluta om lämpliga åtgärder när en incident upptäckts (Cichonski, Millar, Grance, & Scarfone, 2012; ENISA, 2010; Sommestad & Hunstad, 2013). För att studera logganalysförmåga har begreppet i projektet ÖvExCy delats upp i processerna informationsinsamling, automatisk analys och manuell analys (Sommestad & Holm, 2015), vilket illustreras i Figur 1.



Figur 1. Översikt över logganalysarbete och den input och output som hanteras.

Som figuren visar behöver logganalytiker under den manuella analysen ha tillgång till händelser och tillstånd, larm från automatiska analysverktyg, bra förståelse för det egna systemet och kunskap om cybersäkerhet. Med utgångspunkt från detta försöker logganalytikerna identifiera hot mot systemet och lämpliga åtgärder för att möta dessa hot. Lämpliga åtgärder kan till exempel vara ändrade systemkonfigurationer, uppdaterade mjukvaror och att maskiner tas ur drift. Ibland slutar analysen med återkoppling till de som konfigurerar informationsinsamling och automatisk analys. Till exempel då något visat sig vara ett falsklarm eller då information som behövs för analysen saknas. I många fall produceras också incidentbeskrivningar i from av rapporter eller meddelanden till andra logganalytiker och externa intressenter.

1.2 Incidentbeskrivningar

När en cybersäkerhetsincident upptäcks så krävs lämpliga åtgärder, men det är också viktigt att rapportera det som inträffat. Rapporteringen kan vara mer eller mindre omfattande och det är viktigt att information noteras och loggas i samband med att incidenten sker för att undvika att viktig information glöms bort. Denna typ av incidentbeskrivningar kan göra det möjligt att identifiera samband och skapa förståelse för hur enskilda händelser ingår som en del i ett större angrepp, till exempel ett lågintensivt angrepp som pågår under lång tid, eller flera samtidiga angrepp mot flera delar av en organisation. Eftersom det inte finns några vedertagna standarder för hur en incidentbeskrivning ska se ut, har en del av arbetet i ÖvExCy inriktats mot detta och sökt svar på frågan: *Vilka informationselement är lämpliga att dokumentera i logganalysarbete som syftar till att stödja incidenthantering?*

Projektet ÖvExCy har även tidigare arbetat med frågor kopplade till situations-medvetande och incidentbeskrivningar. Under 2015 genomfördes intervjuer med domänexperter så att en målinriktad uppgiftsanalys och hierarkisk uppgiftsanalys kunde genomföras (Lif, Holm, Sommestad, Granåsen, & Westring, 2016). Vilken information incidenthanterare behövde ha koll på för att erhålla god situationsmedvetande har även dokumenterats i en artikel (Lif, Granåsen, & Sommestad, 2017) och diskuterats med forskare på en internationell konferens inom cybersäkerhet[1]. Denna rapport presenterar ett konkret förslag på informationselement att inkludera i en incidentbeskrivning, baserat på tidigare arbete, och undersöker i vilken omfattning föreslagna informationselement används av praktiker. Dessutom undersöks hur elementen samvarierar med kvaliteten på incidentbeskrivningarna och deltagarnas subjektiva upplevelser av att använda elementen. Slutligen diskuteras framtagandet av incidentbeskrivning,

[1] http://www.c-mric.com/

bland annat utifrån designforskningens (eng. ”*design science*”) sju riktlinjer (Hevner, March, Park, & Ram, 2004).

1.3 Rapportöversikt

Kapitel 2 beskriver litteratur kopplad till incidentbeskrivningar och det tidigare arbete som utförts i projektet om incidentbeskrivningar. Kapitlet avslutas med en presentation av de informationselement som bedöms lämpliga att inkludera i en incidentbeskrivning av enklare typ. Kapitel 3 redovisar ett empiriskt test där dessa element används i en cybersäkerhetsövning med fokus på incident-hantering. Testet utvärderar hur användarna upplever beskrivningsformatet, om de klarar av att använda informationselementen och huruvida övningsledningen upplevde incidentbeskrivningarna bättre om fler av informationselementen användes. Kapitel 4 innehåller diskussion och slutsatser med avseende på resultaten från testet.

2 Framtagande av informationselement

Mätning av logganalytikers situationsmedvetande har gjorts tidigare i projektet (Lif m.fl., 2016). Detta har gett en översikt över vilka element som bör inkluderas vid mätning av situationsmedvetande och därmed också viss kunskap om vilka informationselement som bör inkluderas i incidentrapporter (Lif m.fl., 2016). För att ytterligare öka kunskapen om incidentrapportering har fortsatt utvecklingsarbete genomförts där incidentbeskrivningsförslag från bland andra STIX (2017), VERIS (2017) och NIST (Cichonski m.fl., 2012) analyserats och använts som utgångspunkt för att komplettera tidigare genomfört arbete inom projektet.

2.1 Informationselement för situationsmedvetande

Situationsmedvetande är ett väletablerat område inom forskning om mänskliga faktorer (eng. *human factors*). Det finns flera definitioner av situationsmedvetande. Nedan presenteras en svensk översättning av en av de mer etablerade definitionerna av Endsley (1995):

> *”Uppfattningen av element i miljön inom given tid och rum, förståelsen av deras betydelse och förmågan att predicera deras tillstånd inom en snar framtid.”*

Med utgångspunkt från denna definition kan situationsmedvetande inom cybersäkerhet beskrivas som att upptäcka, förstå och predicera hur en incident utvecklas över tid. Att klargöra vilka informationselement som bör inkluderas i olika situationer är centralt för förståelsen av situationsmedvetande inom cybersäkerhet. Även om forskningen om situationsmedvetande inom cybersäkerhet har intensifierats under senare år (Ben-Asher & Gonzalez, 2015; Bowen, Stolfo, & Devarajan, 2012; Boyce m.fl., 2011; D’Amico, Whitley, Tesone, O’Brien, & Roth, 2005; Dutt & Gonzalez, 2011; Mahoney m.fl., 2010; Mancuso, Strang, Funke, & Finomore, 2014; Tenney & Pew, 2006) är området fortfarande dåligt definierat och det är fortfarande oklart vilka element som situationsmedvetande kan brytas ner i för att förtydliga, konkretisera och förstå dess innebörd. I vissa vetenskapliga publikationer (Mahoney m.fl., 2010) är informationselementen angivna på en hög och abstrakt nivå, vilket innebär att beskrivningen från ett tekniskt perspektiv blir otydlig.

Barford m.fl. (2010) anser att situationsmedvetande inom cybersäkerhet täcker sju aspekter: nuvarande läge, attackens skadeverkan, hur läget utvecklas, motståndarens beteende, varför och hur läget uppstod och hur läget kan utvecklas över tid. Mahoney m.fl. (2010) har genom uppgiftsanalys identifierat nio olika aspekter av situationsmedvetande och listar vad användaren behöver vara

medveten om: hälsa, aktivitet, anslutningar, förändring, datakälla, konsekvent, kommunikation, sårbarhetsomfattning och social/organisation/beteende. Dressler m.fl. (2014) anser att ett system som ska ge situationsmedvetande bör innehålla sex informationsklasser: hotmiljö, skadlig aktivitet, sårbarheter, nyckelterräng, operationell färdighet och pågående operationer. Även om dessa sex informationsklasser ger en viss förståelse av hur situationsmedvetande kan brytas ner så behöver klasserna definieras ytterligare. D'Amica m.fl. (2005) föreslår en mer tekniskt konkret beskrivning innehållande bland annat IP-adresser, portnummer/protokoll och paketinnehåll.

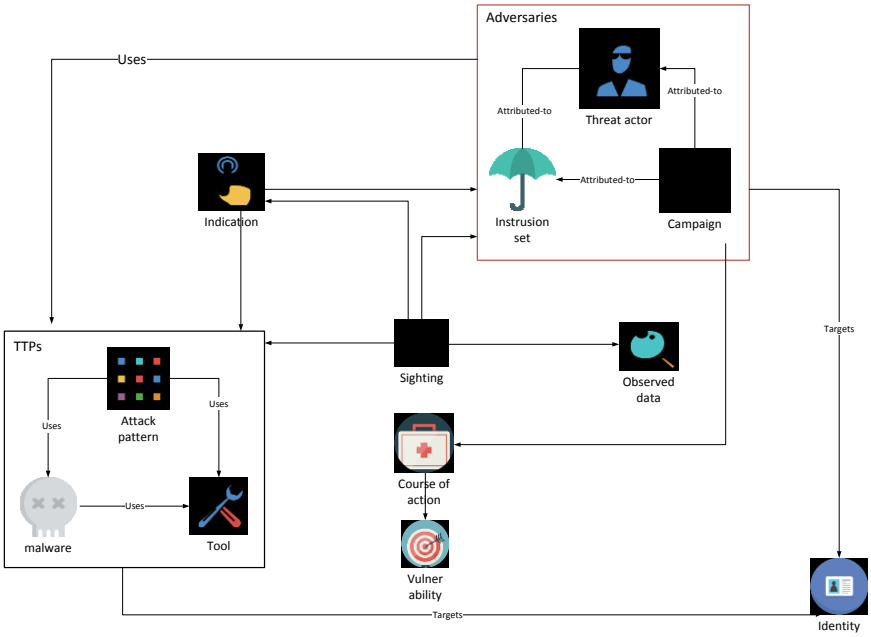
Litteraturen kopplad till situationsmedvetande inom cybersäkerhet innehåller alltså många definitioner och visar att det finns spridda idéer om vilka element som situationsmedvetande ska brytas ner i. Vissa ser situationsmedvetande som något övergripande och abstrakt; andra ser det som något konkret och ofta som tekniskt. Spretigheten är också något som rent allmänt gäller forskningen på situationsmedvetande i cybersäkerhetssammanhang (Franke & Brynielsson, 2014).

2.2 Informationsmodeller för incidentbeskrivningar

Det finns flera förslag på hur incidenter ska beskrivas som tagits fram av standardiseringsorgan, intresseorganisationer och myndigheter. Nedan redovisas tre förslag, i tur och ordning från incidenthanteringsstandarden STIX, incidentdatabasen VERIS och incidenthanteringsguiden från NIST.

2.2.1 Structured Threat Information Expression

Structured Threat Information Expression (STIX) är en datamodell för inrapportering av incidenter där informationen struktureras efter förutbestämda mallar för att kunna spridas mellan olika intressenter (Figur 2).



Figur 2. Förenklad STIX-arkitektur med ikoner[2345].

Enligt STIX finns det flera domänobjekt (specificerade objekt som beskriver incidenter) som kan användas som indikatorer för vad logganalytiker behöver analysera och samla information om i samband med en incident. Logganalytikern övervakar datornätverket och söker (*eng. sighting*) efter misstänkt skadlig kod. Motståndaren beskrivs genom att ange vem som ligger bakom attacken (*eng. threat actor*), om attacken ingår i ett större mönster av attacker (*eng. campaign*) och motståndarens resurser och beteenden (*eng. intrusion set*). Utifrån kunskap om bland annat motståndaren söks efter vilken person, grupp eller organisation som ligger bakom attacken (*eng. identity*), vad som behöver göras för att förhindra att attacker sker eller stoppa en pågående attack (*eng. course of action*). Detta innebär ofta att säkerställa att sårbarheter (*eng. vulnerability*) inte existerar i det egna nätet. För att upptäcka och kartlägga vem som ligger bakom attacken samlas även information om motståndarens taktik, teknik eller procedur (*eng. TTP - tactic, technique or procedure*), som innehåller attackmönster (*eng. attack pattern*), verktyg (*eng. tool*) och skadlig kod (*eng. malware*) som används. Det anges hur man kan upptäcka angreppet (*eng. indicator*) och vilken informations-insamling som krävs (*eng. observed data*). De informationselement som i STIX

[2] Frost & Lapin (2017). http://smallicons.net/.
[3] Langela (2017). http://www.manuelalangella.com
[4] http://www.smashingmagazine.com/2013/11/29/freebie-smallicons-icon-set/
[5] http://www.iconshock.com

betecknas domänobjekt anges i Tabell 1 tillsammans med antalet egenskaper som respektive domänobjekt består av.

Tabell 1. Domänobjekt med gemensamma och specifika egenskaper.

Domänobjekt	Antal gemensamma egenskaper	Antal specifika egenskaper
Attack pattern	10	3
Campaign	10	6
Course of action	10	3
Identity	10	5
Indicator	10	6
Intrusion set	10	8
Malware	10	3
Observed data	10	4
Report	10	4
Threat actor	10	10
Tool	10	4
Vulnerability	10	2

STIX tolv domänobjekt beskrivs genom innehåll och relationer till andra objekt (de streck som visas i Figur 2). Domänobjekten innehåller tio gemensamma egenskaper (*type, id, created_by_ref, created, modified, revoked, labels, external_references, object_marking_refs, granular_markings*) som ska noteras. Därutöver har varje domänobjekt specifika egenskaper. Till exempel har *attack pattern* krav på att användaren ska ange namn, textbeskrivning och var i *kill-chain* (Lockheed Martin, 2017) attackmönstret används. Tolv domänobjekt med tio gemensamma egenskaper innebär 120 fält att fylla i, därtill tillkommer 58 specifika egenskaper (3-10 per objekt) och relationer mellan objekt. Incident-beskrivningar gjorda med STIX blir alltså ofta innehållsrika.

2.2.2 Vocabulary for event recording and incident sharing

Vocabulary for Event Recording and Incident Sharing (VERIS) är ett ramverk som består av en uppsättning mätvärden för att skapa ett standardiserat sätt att beskriva incidenter. Idén är att börja enkelt med sju mätvärden: år, månad, dag, vem som upptäckt incidenten, vad som skett och hur det skett. Sedan används två nivåer med fält för information (som i VERIS betecknas *enumerations*). På den första nivån bedöms om det var en riktig attack eller ej och hur attacken upptäcktes. På den andra nivån finns fälten för *Actor*, *Action*, *Asset, Attribute* (4A) och ytterligare detaljer som sammanlagt innehåller 74 fält. I VERIS beskrivs dessutom ett schema för dokumentation som delas in i *incident tracking*

(32 fält), *victim demographics* (45 fält), *discovery & response* (46 fält) och *impact assessment* (30 fält).

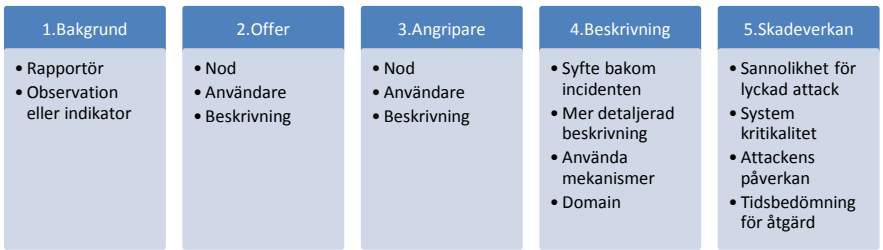
2.2.3 Computer security incident handling guide

Computer security incident handling guide (Cichonski m.fl., 2012), utgiven av U.S. National Institute of Standards and Technology (NIST), syftar till att stötta organisationer i deras arbete med incidenthantering på ett ändamålsenligt och effektivt sätt. Guiden innehåller grundläggande och incidenthanterare element. De grundläggande elementen delas vidare upp i information om rapportören (6 element), detaljer om incidenten (11 element) och generella kommentarer. Det finns dessutom sju punkter kopplade till incidenthanterare. NIST-guiden är mer övergripande och innehåller färre formaliserade detaljer än STIX och VERIS. Detaljerna om incidenten ges istället i form av textuella beskrivningar, t.ex. av vilka resurser som påverkats, hur incidenten upptäcktes och vilka motåtgärder som använts.

2.3 Framtaget förslag för incidentbeskrivningar

Det finns en begränsad samsyn om vilka informationselement som behövs för att rapportera en lägesbild i cybersäkerhetssammanhang, vilket ovanstående genomgång visar. Vissa förslag inkluderar till exempel abstrakta informationselement som hälsa medan element såsom IP-adresser är mer konkreta. De mallar som finns att tillgå i guider och standarder inkluderar många detaljer (över 100 attribut) eller detaljrika textuella beskrivningar av incidenterna. Detta är i sig naturligt eftersom det finns mycket information som kan samlas in och inkluderas i en incidentbeskrivning. De informationsmodeller som STIX och VERIS använder är tänkta att fånga den information som finns tillgänglig efter att en incident har hanterats och loggar analyserats på djupet. De är alltså inte tänkta att beskriva de informationselement som ska inkluderas i anteckningar som förs under tiden en incident analyseras eller då lägesinformation ska kommuniceras mellan logganalytiker. Sådana incidentbeskrivningar behöver av praktiska skäl vara enkla att skapa och läsa.

Baserat på tidigare arbete som genomförts inom projektet (Lif m.fl., 2016) med utgångspunkt i STIX, VERIS och NIST har ett förslag utarbetats avseende vilka informationselement som bör inkluderas i incidentrapporter. Förslaget innehåller fem kategorier: bakgrund, offer, angripare, beskrivning och skadeverkan (Figur 3). Dessa kategorier innehåller mellan två och fyra informationselement vardera, vilket summerar till totalt 16 stycken element.



Figur 3. Fem kategorier med sammanlagt 16 informationselement för incidentrapportering.

En översiktlig beskrivning av hur kategorierna kopplar till STIX, VERIS och NIST-guiden ges i Tabell 2.

Tabell 2. Relation mellan ramverken STIX, VERIS, NIST och de fem kategorier med informationselement i framtaget förslag till incidentrapport.

Kategori	STIX	VERIS	NIST
Bakgrund	×	×	×
Offer		×	×
Angripare	×	×	×
Beskrivning	×	×	×
Skadeverkan		×	×

STIX, som innehåller informationselement kopplade till tre av kategorierna, fokuserar på attacken och vad som sker men inkluderar inte det egna nätet och vilken skadeverkan en incident fått eller potentiellt kan få. VERIS och NIST innehåller informationselement kopplade till samtliga kategorier.

Innehållet i den föreslagna incidentbeskrivningsmallen stämmer väl överens med innehållet i granskade ramverk. Men det framtagna förslaget är förenklat för att kunna användas under övning och i verksamheter där det finns begränsat med tid att skriva incidentbeskrivningar. Syftet var inte att utveckla en mall i sig utan att undersöka vilka informationselement som bör inkluderas i en incidentbeskrivningar. Denna information kan sedan användas för att anpassa mallar för incidentbeskrivning bland annat för Försvarsmaktens analytiker.

3 Utvärdering av informationselement

Detta kapitel beskriver en utvärdering som gjordes av en incidentbeskrivningsmall under incidenthanteringsövningen iPILOT (Polisen, 2017). Mallen innehöll de informationselement som beskrivs i avsnitt 2.3 och sökte svar på tre frågor:

1. **I vilken omfattning används de sexton föreslagna informationselementen av logganalytiker under övningen?**
   En användbar incidentbeskrivningsmall innehåller element som är relevanta och som är möjliga att svara på.
2. **I vilken utsträckning samvarierar användningen av de sexton elementen med den kvalitet övningsledningen ansåg att rapporterna hade?**
   För att informationselementen ska tillföra värde ska de uppfattas som bra och innehållsrika av övningsledningen när de används.
3. **Hur upplevde logganalytikerna att det var att använda incidentbeskrivningsmallen?**
   Det är önskvärt att logganalytikerna finner innehållet i incidentbeskrivningsmallen meningsfull.

Det finns flera faktorer som kan tänkas påverka resultatet men som inte direkt har med informationselementen att göra. Eftersom iPILOT var en övning är träningseffekt ett sådant uppenbart exempel, det vill säga att övningsdeltagare behöver tid för att lära sig upptäcka angrepp, använda mallen och producera innehållsrika beskrivningar. Detta testades genom att jämföra användningen av mallen för incidentbeskrivning i början och slutet av övningen. En ytterligare faktor som kan tänkas påverka resultatet är användbarheten i det mjukvaruverktyg som mallen implementerades i, varför deltagarnas uppfattning om detta verktyg också samlades in under övningen.

Nedan beskrivs övningen iPILOT, deltagarna i övningen, den tekniska övnings-miljön, den mall där informationselementen var inbäddade och resultatet av de mätningar som gjordes.

3.1 iPILOTs syfte

Det övergripande syftet med övningen iPILOT var att öka incident-hanteringsförmågan och bredda det personliga kontaktnätet för individer i funktioner som involveras vid en allvarlig cyberattack mot kärntekniska anläggningar (Polisen, 2017). Incidenthanteringsförmågan övades genom att deltagarnas uppgift var att säkerställa driften hos det IT-system som styrde ett simulerat kolkraftverk och samtidigt upptäcka intrång och felkonfigurationer i

det egna datornätverket. Kontaktnätsuppbyggnad möjliggjordes genom att låta personer från olika organisationer arbeta i nykomponerade grupper med personer från andra organisationer. Övningen genomfördes under fyra dagar med introduktion och utbildning under dag 1, genomförande under dag 2-3 och utvärdering under dag 4. Då personalen som övades primärt jobbar med IT inom kärnkraftsindustrin men scenariot var drift av ett kolkraftverk finns en risk att övningen upplevdes konstlad av deltagarna. Nedanstående avsnitt ger ytterligare detaljer om övningens deltagare, tekniska miljö, incidentbeskrivningsmallen och de tester som utfördes.

3.2 Deltagare

Deltagarna under övningen kom från Strålsäkerhetsmyndigheten, Svenska kraftnät, Polisen, Myndigheten för samhällsskydd och beredskap (MSB), Säkerhetspolisen (SÄPO), Forsmarks Kraftgrupp AB (FKA), Oskarshamnsverket (OKG), Ringhals AB (RAB), Svensk Kärnbränslehantering AB (SKB) och Westinghouse Electric Sweden AB (WSE). De flesta av deltagarna är vana att arbeta inom det kärntekniska området. Sammanlagt deltog 30 personer från dessa organisationer och de arbetade under övningen i fem mixade grupper där de inte kände de andra i gruppen innan övningen. Även om deltagarna var vana vid arbete med incidenthantering så var deras erfarenhet begränsad när det gäller att skriva incidentbeskrivningar.

3.3 Teknisk övningsmiljö

Övningen genomfördes i Katastrofmedicinskt centrums lokaler i Linköping där varje deltagande grupp hade ett rum till förfogande. Den tekniska infrastrukturen i övningen realiserades av FOI:s cyberträningsanläggning *Cyber Range And Training Environment* (CRATE). CRATE består av cirka 750 servrar i ett kluster med utrustning för kommunikation internt och mot Internet (Sommestad, 2015). Med hjälp av dessa noder byggdes ett simulerat nätverk bestående av virtuella datorer som är tänkta att efterlikna verkliga cybermiljöer. I denna övning bestod cybermiljö av ett datornätverk som representerade ett mindre företag inom kraftproduktion.

Varje deltagare hade en bärbar dator till sitt förfogande med operativsystemet Ubuntu som baseras på Linuxkärnan och olika verktyg för att möjliggöra upptäckt av incidenter. Verktygen möjliggjorde att deltagarna kunde genomföra: skanning av de egna nätverken[6], få grafisk framställan av nätverkstrafiken[7],

[6] https://linux.die.net/man/1/arp-scan
[7] http://etherape.sourceforge.net/

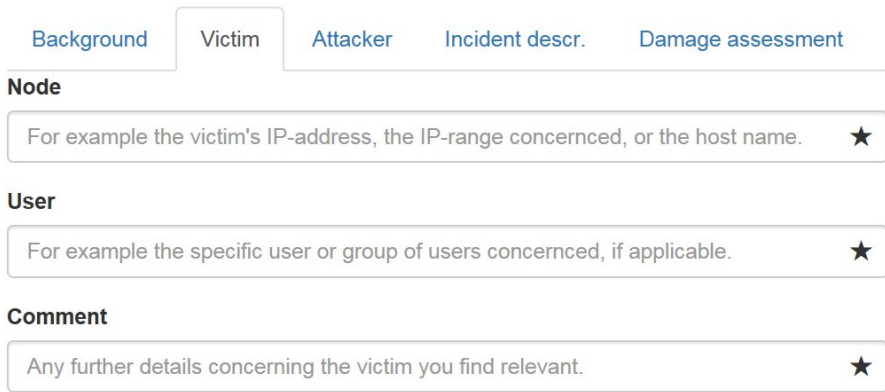
övervaka datorstatus[8], intrångsdetektion[9], trafikavlyssning[10], analys av nätverks-trafik[11] och skanning av sårbarheter[12]. Deltagarna hade dessutom verktyg för att rapportera incidenter (se nedan) och de besvarade webbaserade enkäter.

Attackerna mot de försvarande grupperna genomfördes skriptat av spelledningen med verktyget *Scanning, Vulnerabilities, Exploits and Detection* (SVED) som är en programvara för att på ett automatiserat sätt angripa noder i datornätverk under övningar genom att utnyttja sårbarheter (Holm & Sommestad, 2016).

De fem grupperna arbetade separat och tilläts inte samarbeta med de andra grupperna. Grupperna hade identiska förutsättningar avseende den tekniska miljön och utsattes för samma attacker vid samma tidpunkt under de två dagarna.

3.4 Incidentbeskrivningar

Utifrån de fem kategorierna och tillhörande informationselement (Figur 3) skapades en webbaserad mall för incidenthantering som totalt innehöll 16 fält för inmatning av information. Mallen presenteras i sin helhet i Bilaga 1 och exemplifieras i Figur 4.



Figur 4. Exemplifiering av mall för incidenthantering för kategorin offer (victim).

Mallen fanns tillgänglig i det webbaserade verktyget *CRATE Exercise Control* (CEC) som både deltagare och spelledning hade tillgång till. Deltagarnas uppgift var att upptäcka incidenter, samla information och efter bästa förmåga använda mallen för incidentbeskrivning. Spelledningens uppgift var att granska och

[8] http://freecode.com/projects/gtkpinger
[9] https://github.com/Snorby/snorby
[10] https://linux.die.net/man/8/tcpdump
[11] https://www.wireshark.org/
[12] https://nmap.org/zenmap/

bedöma kvaliteten på deltagarnas beskrivningar enligt ett poängsystem. Poängbedömningen gjordes enligt ett fördefinierat poängsystem där viss information eftersöktes. Detta poängsystem har tagits fram oberoende av informationselementen och det finns ingen direkt överenstämmelse mellan vilka fält i mallen som besvarats korrekt för respektive incident och den fördefinierade poängbedömningsmallen. Riktlinjerna för poängbedömning av respektive incident definierades av spelledningen före övningens start. I Tabell 3 ges två exempel på incidenter och hur deltagarnas incidentbeskrivningar poängbedömdes av spelledningen.

Tabell 3. Exempel på två incidenter och mallar för poängbedömning.

Namn	Beskrivning	Poängbedömning
Bittorrent i nätverket.	Klienten µTorrent körs av användare för att ladda ner och dela material (ev. copyrightskyddat) och även malware laddas ner.	Upptäckt med Snort är avgörande för en bra analys (60 poäng). Beskrivning av påverkade datorer (60 poäng), användare (40 poäng) och tracker (40 poäng) måste beskrivas för att 200 poäng ska erhållas.
DDoS mot företagets webserver	En DDoS-attack startas mot webserver.	Upptäckt av DDoS inom 15 minuter från initierad attack ger 120 poäng, efter 15 minuter erhålls 60 poäng. Upptäckt av attackerande IP-adresser ger ytterligare 40 poäng. Förslag på att blockera IP-nummer i brandväggen eller annan liknande lösning ger ytterligare 40 poäng.

3.5 Resultat

De fem grupperna skickade sammanlagt in 172 incidentbeskrivningar. Grupp ett lämnade in 22 beskrivningar, grupp två 33 beskrivningar, grupp tre 23 beskrivningar, grupp fyra 73 beskrivningar och grupp fem 21 beskrivningar. Dessa beskrivningar analyseras här avseende användning av informationselement, beskrivningarnas kvalitet och upplevt värde av informationselementen.

3.5.1 Användning av informationselement

I vilken omfattning föreslagna informationselement används (fråga 1) ges i Tabell 4. Andelen ifyllda fält varierar kraftigt mellan olika informationselement. Bakgrund (informationselement 1) fylldes i bra, med undantag av rapportörens

namn vilket utelämnades i mer än hälften av beskrivningarna dag ett. I informationselementet för beskrivningen av offer (informationselement 2) rapporterades ofta angripen nod, men betydligt mer sällan vilken användare det gäller och den detaljerade beskrivning som efterfrågades. En anledning till att siffrorna är låga för offrets användare är att det inte alltid var möjligt att fylla i detta fält eller att det helt enkelt var irrelevant. Deltagarna gav sällan en detaljerad beskrivning av offret, t.ex. vilken systemfunktion det levererade. Eventuellt beror detta på att sådan förståelse kräver en mer omfattande analys som inte bedömdes prioriterad i övningen. Angripare (informationselement 3) användes sällan. Också detta kan tänkas bero på tidsbrist och att incident-hanterarna inte hann analysera bakgrunden till angrepp. Den mer detaljerade beskrivningen av angreppets utförande (informationselement 4) fylldes i på en förhållandevis hög nivå givet den relativt stressade situation deltagarna befann sig i och skadeverkningar (informationselement 5) fylldes i mycket bra.

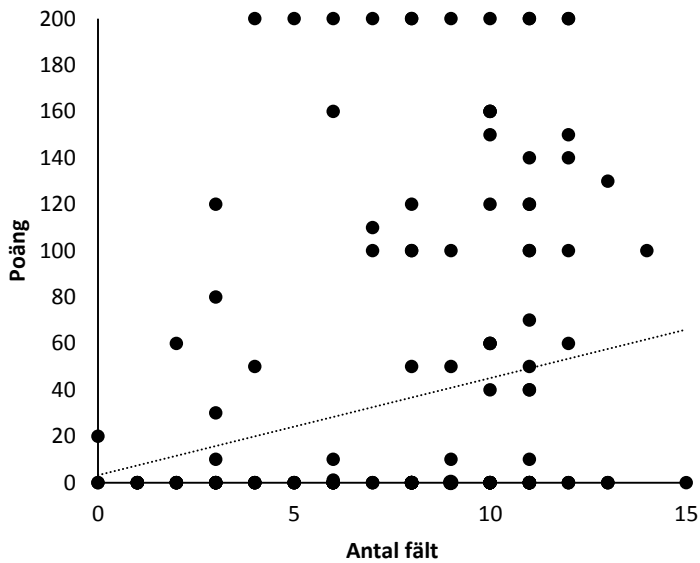
Tabell 4. Andel ifyllda fält för incidenthanteringsrapporterna.

Kategori	Informationselement	Ifyllnadsgrad dag 1	Ifyllnadsgrad dag 2
1.Bakgrund	Rapportör	48%	94%
	Observationer / indikationer	92%	98%
2.Offer	Nod	77%	91%
	Användare	18%	30%
	Beskrivning	17%	37%
3.Angripare	Nod	25%	56%
	Användare	5%	19%
	Beskrivning	6%	24%
4.Beskrivning	Syfte	60%	86%
	Mer detaljerad beskrivning	50%	60%
	Använda mekanismer	49%	52%
	Domän	46%	54%
5.Skadeverkan	Sannolikhet för lyckad attack	61%	73%
	System kritikalitet	64%	83%
	Attackens påverkan	62%	81%
	Tidsbedömning för åtgärd	62%	84%

3.5.2 Beskrivningarnas kvalitet

Det finns ett svagt men tydligt samband mellan användningen av fälten och den poäng som gavs. Pearsons produktmomentkorrelationskoefficient (Hays, 1994) mellan antalet fält som användes och antalet poäng som gavs var $r = 0,22$ och sambandet var statistiskt säkerställt ($p = 0,003$). Figur 5 illustrerar kopplingen mellan antal fält och tilldelade poäng. Lutningen på strecket illustrerar

regressionslinjen och spridningen illustrerar det förhållandevis svaga sambandet. I figuren syns också tydliga tak- och golveffekter. Det vill säga att många rapporter fått antingen noll poäng eller maximala 200 poäng. Det är möjligt att det statistiska sambandet skulle vara starkare med ett poängsystem som gett minuspoäng vid direkt felaktiga rapporter och som gett mer än 200 poäng för excellenta rapporter. Det indikeras också av att Pearsons produktmomentkorrelationskoefficient är 0,34 om endast de rapporter som getts 1-199 poäng tas med är i analysen.



Figur 5. Antalet fält som används i rapporterna och antalet tilldelade poäng. Punkterna är färgkodade så att en ljusgrå punkt motsvarar en enskild rapport medan ju mörkare punkter desto fler rapporter förekommer i mätningen med samma antal fält och poäng.

Antalet rapporter (172) är inte tillräckligt många för att med någon säkerhet göra uttalanden om vilka fält som har störst betydelse. En regressionsmodell med poäng som beroende variabel och fälten som oberoende variabler indikerar att de rapporter som inkluderade information om angriparen, observationer och tillgångens kritiskhet fick i regel fler poäng av övningsledningen. Detta håller även då antalet fält inom respektive kategori används som oberoende variabel. Som Tabell 5 visar fick deltagarna i snitt 45,5 poäng för varje fält som låg i kategorin bakgrund (rapportör och observation) och 5,6 poäng för de fält som låg i kategorin angripare (t.ex. IP-adressen). De flesta av sambanden mellan antal fält och poäng är dock inte statistiskt säkerställda och det ska noteras att det finns flera tänkbara störkällor. Ibland använde deltagarna fälten på ett felaktigt sätt,

och t.ex. skrev incidentbeskrivningar i rapportörsfältet. Ibland fylldes några fält i med inkorrekta värden och därför inte fick några poäng, till exempel då de agerade på falsklarm.

Tabell 5. Antalet poäng som kan härledas till fält i respektive kategori användes. Endast fältet bakgrund är statistiskt signifikant.

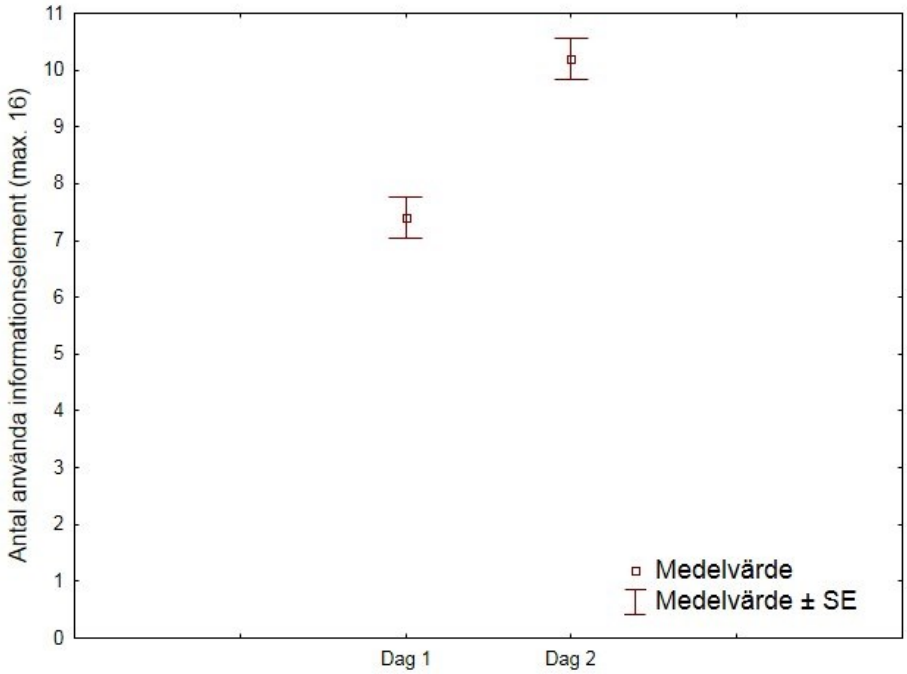
Kategori	Poäng per fält
Angripare	5,6
Bakgrund	45,5
Beskrivning	-1,7
Offer	3,2
Skadeverkan	2,8

3.6 Upplevt värde av informationselementen

För att besvara huruvida värdet av respektive informationselement var meningsfullt fick deltagarna besvara enkätfrågor på en sjugradig skala. Det fanns dessutom en öppen fråga där deltagarna i text kunde ge övriga kommentarer. Ett lågt värde var alltid negativt och ett högt värde positivt, t.ex. 1=mycket låg och 7=mycket hög. Deltagarnas skattningar av innehållet i incidentbeskrivningarna var i snitt 4,3. Detta värde indikerar att det krävs fortsatt arbete med att anpassa vilka informationselement som bör användas till deltagare med samma eller liknande bakgrund som i denna övning. En vanligt förekommande kommentar från deltagarna var att de upplevde att de behövde rapportera in mycket information men vid diskussion med en av grupperna framkom att flera av dem vanligen använde mer detaljerade incidentbeskrivningar. En möjlig källa för viss frustration var övningens höga tempo som innebar att de behövde skriva många incidentbeskrivningar under kort tid.

3.6.1 Träningseffekt och upplevelse av rapporteringssystem

Som Tabell 4 visar är det en märkbar skillnad mellan hur elementen användes under dag 1 och 2. T-test visar också att det finns en statistisk säkerställd skillnad ($t = 4{,}7$; $df = 62$, $p < 0{,}001$). Figur 6. illustrerar skillnaden grafiskt. Av allt att döma finns en tydlig träningseffekt.



Figur 6. Genomsnittligt antal ifyllda fält dag ett och dag två med ± 1 standardfel.

Träningseffekten som visas i Figur 6 och manifesterades i mer kompletta beskrivningar påverkade poängsättningen positivt. Den första dagen beskrevs 109 incidenter och grupperna erhöll i snitt 29,8 poäng per inlämnad rapport; den andra dagen beskrevs 63 incidenter och grupperna erhöll i snitt 44,4 poäng per inlämnad beskrivning. Deltagarnas subjektiva skattningar av övningshanteringsverktyget CEC var relativt låga (övergripande medelvärde 3,7; specifikt för incidentbeskrivning 3,4). Då CECs främsta syfte inte är att beskriva incidenter utan att samla all information som behövs för övningsledningens lägesbild på ett ställe så är denna relativt låga användarvänlighet känd och kan dessvärre ha påverkat testets resultat på ett negativt sätt.

4 Diskussion och slutsatser

Arbetet som presenterats i denna rapport utgår från tidigare genomförd litteraturstudie, befintliga ramverk för incidentbeskrivning (främst STIX, VERIS och NIST), tidigare framtaget förslag för mätning av situationsmedvetande för logganalytiker och intervjuer av logganalytiker. Utifrån denna samlade information utarbetades ett konkret förslag på vilka informationselement som bör inkluderas i en incidentbeskrivning.

Ett sätt att bedöma vetenskaplig designforskning inom informationssystem är användandet av de sju riktlinjerna på så kallad designforskning (eng. *design science)* (Hevner, March, Park, & Ram, 2004). Enligt dessa riktlinjer ska en artefakt skapas (riktlinje 1) som löser ett viktigt och relevant problem (riktlinje 2). Artefakten måste sedan utvärderas för att säkerställa dess användbarhet för det angivna problemet (riktlinje 3). För att vara ett meningsfullt designforskningsbidrag måste artefakten antingen lösa ett befintligt problem eller tillhandahålla en effektivare lösning än vad som tidigare presenterats (riktlinje 4). Både konstruktion och utvärdering av artefakten måste göras noggrant (riktlinje 5). Processen genom vilken artefakten utvecklas möjliggör en iterativ process där nya effektiva sätt för att lösa problemet kan uppkomma (riktlinje 6). Resultaten av forskningen ska dessutom presenteras effektivt både till personer med teknikorienterat fokus och till personer i ledningsbefattningar (riktlinje 7).

Studien som presenteras i denna rapport möter riktlinjerna för *design science* på följande sätt:

- Incidentbeskrivningen med de sexton informationselementen som presenteras i denna rapport är utvecklat för att logganalytiker ska kunna använda den i en praktisk situation. Detta är alltså en artefakt som producerats (riktlinje 1).
- Hur incidentbeskrivningsmallar ska konstrueras är ett relevant och aktuellt problem som forskare och organisationer försöker hitta en bra lösning på (riktlinje 2).
- Utvärdering har genomförts (riktlinje 3), men bör upprepas i mer realistiska sammanhang, med professionella incidenthanterare. Dessutom var iPILOT i första hand en övning i att hantera incidenter, och inte en övning i rapportering eller beskrivning av att upptäckta incidenter, vilket begränsade kvaliteten på insamlade data.
- En brist i denna studie, är att det framtagna förslaget inte jämförs med andra alternativa incidentbeskrivningar. Men till skillnad från existerande förslag, till exempel STIX och VERIS, är incidentbeskrivningarna här anpassade för situationer där det inte finns tid att skriva långa utförliga rapporter. Detta fyller ett behov som inte

inkluderas i de mer omfattande ramverken. Det borde alltså innebära en förbättring mot existerande förslag (riktlinje 4).

- Konstruktionen av artefakten (riktlinje 5) har varit noggrann.
- För att säkerställa att rätt informationselement används så har bland annat litteraturstudier och intervjuer med logganalytiker genomförts enligt vedertagna metoder. En tidigare version har också testats i samband med en övning. Utvecklingsarbetet har alltså bedrivits iterativt och gett ny kunskap om vilka informationselement som bör användas (riktlinje 6). Samtidigt kan det inte betraktas som färdigt. Mer forskning krävs för att anpassa incidentbeskrivningarna till olika situationer.
- Resultat och erfarenheter om incidentbeskrivningar som beskrivs i denna rapport kommer att redovisas för beslutsfattare och logganalytiker inom Försvarsmakten för att få ytterligare värdefull återkoppling om värdet av dessa informationselement. Dessutom avses resultaten redovisas på en vetenskaplig konferens med deltagare inom cybersäkerhet under 2018 där deltagarna har mycket god teknisk kompetens. Resultaten kommer därför presenteras för personer med teknikorienterat fokus och personer i ledningsbefattningar (riktlinje 7).

Frågan som i denna studie sökts svar på var: *Vilka informationselement är lämpliga att dokumentera i logganalysarbete som syftar till att stödja incidenthantering?* Detta bröts ner i en litteraturstudie och en utvärdering av i vilken omfattning föreslagna informationselement användes, om elementen samvarierade med kvaliteten på incidentbeskrivningarna och deltagarnas subjektiva upplevelser av att använda elementen.

I vilken omfattning informationselementen används varierar mycket, vilket var förväntat. Informationselement 1 (bakgrund), såsom vem som upptäckt incidenten, vad deltagarna observerat och vilken nod som observerats användes i över 90 % av incidentbeskrivningarna under dag två. Vem som utförde angreppet och beskrivningen av denna användes i betydligt mindre utsträckning, vilket inte är förvånande eftersom det är en betydligt svårare uppgift än att t.ex. beskriva vilka indikationer som fått deltagarna att misstänka en incident. Även om deltagarna kunde identifiera vilken nod som attackerades beskrev de sällan vilken användare som berördes eller gav ytterligare beskrivning av offret. Inte heller detta är förvånande, eftersom det vid vissa typer av incidenter inte var någon särskild användare som var offer för angreppet. Incidentbeskrivningen skapades generellt för att kunna användas till olika incidenter, men det innebar att vissa fält ibland lämnades tomma. Detta framgick även vid diskussion med en av grupperna där de påtalade att det inte alltid gick att använda hela incidentbeskrivningen, vilket sannolikt förklarar deltagarnas något modesta skattning av hur meningsfullt innehållet i incidentbeskrivningarna var.

Elementen samvarierade med kvaliteten på incidentbeskrivningarna. Detta visar att det finns ett samband mellan användningen av fälten och den poäng som gavs. Fortsatt arbete behövs, exempelvis för att bättre förstå vilka fält som har störst betydelse och hur inkorrekt ifyllda beskrivningar påverkade resultatet.

En vanligt förekommande kommentar från deltagarna var att de upplevde att de behövde beskriva in mycket information men vid diskussion med en av grupperna framkom att flera av dem vanligen använde mer detaljerade incidentbeskrivningar. En möjlig källa för viss frustration var övningens höga tempo, som innebar att de behövde skriva många incidentbeskrivningar under kort tid. Att det system som användes för att beskriva incidenterna (CEC) bedömdes som icke användarvänligt kan också vara en faktor som påverkade bedömningen i negativ riktning. Tiden för utbildning i CEC och i synnerhet i hur incidentbeskrivningarna skulle fyllas i var för begränsad. Deltagarna hade behövt mer tid på sig och de hade troligen behövt prova på att fylla i ett antal fiktiva beskrivningar för att vara förberedda vid spelstart. Deltagarnas relativt låga skattning av hur det var att använda incidentbeskrivningen och skattningen av CEC tolkas som att dessa verktyg behöver utvecklas för att inte störa lärandet som bör ske i övningar.

Det är också värt att notera att det fanns tydlig skillnad mellan hur informationselementen användes dag ett och dag två, vilket även hade en påverkan på poängsättningen. Den första dagen beskrevs 109 incidenter och grupperna erhöll i snitt 29,8 poäng per inlämnad beskrivning; den andra dagen beskrevs 63 incidenter och grupperna i snitt erhöll 44,4 poäng per inlämnad beskrivning. En trolig anledning till att antalet inlämnade beskrivningar sjönk från dag ett till dag två är att mer arbete lades på respektive beskrivning. Detta styrks också av att rapporternas förbättrade kvalitet från dag ett till dag två.

Den övergripande bedömningen av den framtagna förenklade incidentbeskrivningen är positiv såtillvida att den är användbar under övningar men som den redovisade träningseffekten indikerar så gäller det under förutsättning att deltagare tränas mer inför övningsstart än vad som var fallet under iPILOT. Huruvida incidentbeskrivningen kan användas av logganalytiker i civila sammanhang och i Försvarsmakten är inte undersökt under denna övning och kan därför inte besvaras i denna rapport. Förhoppningen är att incidentbeskrivningen kan användas som ett första steg i situationer där den viktigaste informationen ändå måste rapporteras på ett systematiskt sätt under stressade förhållanden. Det kan t.ex. vara i situationen där en spanare först upptäcker en misstänkt incident och sedan lämnas över incidentbeskrivningen för djupare analys till en analytiker. Spanaren behöver då inkludera viss grundläggande information i incidentbeskrivningen, men denna kan sedan kompletteras av analytikern som kan avsätta betydligt mer tid till den aktuella incidenten.

5 Referenser

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., … Yen, J. (2010). Cyber SA: Situational Awareness for Cyber Defense. I S. Jajodia, P. Liu, V. Swarup, & C. Wang (Red.) (s. 3–14). London: Springer. https://doi.org/10.1007/978-1-4419-0140-8_1

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61. https://doi.org/10.1016/j.chb.2015.01.039

Bowen, B. M., Stolfo, S. J., & Devarajan, R. (2012). Measuring the Human Factor of Cyber Security.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human Performance in Cybersecurity: A Research Agenda. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *55*(1), 1115–1119. https://doi.org/10.1177/1071181311551233

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology*.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *49*(3), 229–233. https://doi.org/10.1177/154193120504900304

Dressler, J., Bowen, C. L., Moody, W., & Koepke, J. (2014). Operational data classes for establishing situational awareness in cyberspace. I *International Conference on Cyber Conflict, CYCON*. https://doi.org/10.1109/CYCON.2014.6916402

Dutt, V., & Gonzalez, C. (2011). Cyber situation awareness: Modeling the security analyst in a cyber-attack scenario through instance-based learning. I *20th Annual Conference on Behavior Representation in Modeling and Simulation 2011, BRiMS 2011*.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

ENISA. (2010). *Good practice guide for incident handling*. Hämtad från file:///C:/Users/patand/Downloads/ENISA_Cyber_Europe_2010_report.pdf

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Hays, W. (1994). *Statistics* (5th uppl.). New York: Ted Buchholz.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1. *Design Science in IS Research MIS Quarterly*, *28*(1), 75–105. Hämtad från https://pdfs.semanticscholar.org/fa72/91f2073cb6fdbdd7c2213bf6d776d0ab411c.pdf

Holm, H., & Sommestad, T. (2016). SVED: Scanning, Vulnerabilities, Exploits and Detection. I *MILCOM 2016 - 2016 IEEE Military Communications Conference* (s. 976–981). IEEE. https://doi.org/10.1109/MILCOM.2016.7795457

Lif, P., Granåsen, M., & Sommestad, T. (2017). Development and validation of technique to measure cyber situation awareness. I *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (s. 1–8). IEEE. https://doi.org/10.1109/CyberSA.2017.8073388

Lif, P., Holm, H., Sommestad, T., Granåsen, M., & Westring, E. (2016). *Genomförd försöksverksamhet inom logganalys för cybersäkerhet* (No. FOI-R--4328--SE). Linköping, FOI. Hämtad från https://intranet.foi.se/rapportsammanfattning?reportNo=FOI-R--4328--SE

LockheedMartin. (2017). Cyber Kill Chain® · Lockheed Martin. Hämtad 15 februari 2017, från http://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). A cognitive task analysis for cyber situational awareness. I *Proceedings of the Human Factors and Ergonomics Society* (Vol. 1). https://doi.org/10.1518/107118110X12829369201115

Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014). Human Factors of Cyber Attacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*(1), 437–441. https://doi.org/10.1177/1541931214581091

Newhouse, B., Keith, S., Scribner, B., & Witte, G. (2017). *Draft NIST SP 800-181, NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Eduction (NICE)*.

Polisen. (2017). EU:S FOND FÖR INRE SÄKERHET. Hämtad 09 november 2017, från https://polisen.se/PageFiles/526097/Nyhetsbrev-1-ISF-2017.pdf

Sommestad, T. (2015). *STO-MP-IST-133 Experimentation on operational cyber security in CRATE*.

Sommestad, T., & Holm, H. (2015). *Variabler av vikt för förmågan att analysera cybersäkerhetsloggar (FOI-R--4126--SE)*. Linköping, Sweden.

Sommestad, T., & Hunstad, A. (2013). Intrusion detection and the role of the system administrator. *Information Management & Computer Security*, *21*(1), 30–40. https://doi.org/10.1108/09685221311314400

STIX. (2017). STIX Whitepaper | STIX Project Documentation. Hämtad 24 mars 2017, från http://stixproject.github.io/getting-started/whitepaper/

Tenney, Y. J., & Pew, R. W. (2006). Situation Awareness Catches On: What? So What? Now What? *Reviews of Human Factors and Ergonomics*, *2*(1), 1–34. https://doi.org/10.1177/1557234X0600200102

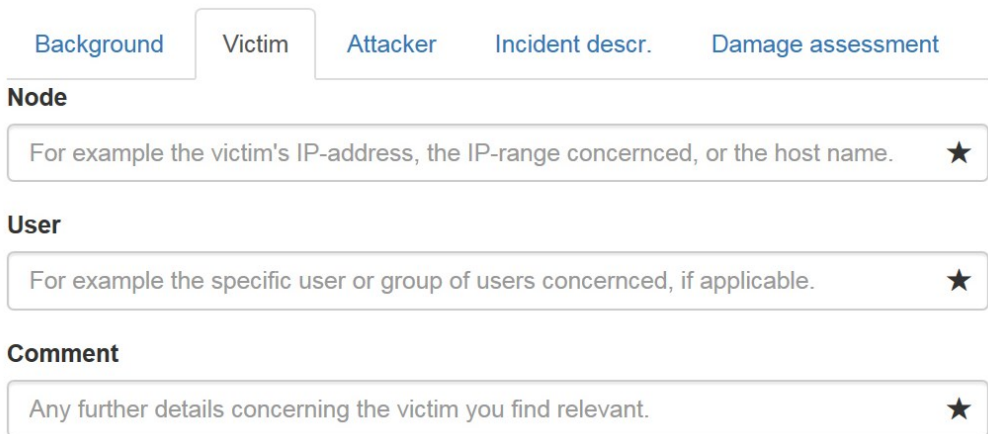
VERIS. (2017). The VERIS Framework. Hämtad 13 november 2017, från http://veriscommunity.net/

Bilaga 1. Mall för incidenthantering

Mallen för incidentbeskrivning bestod av fem kategorier (*background, victim, attacker, incident description & damage assessment*). Varje kategori innehöll informationselement. Sammanlagt användes 16 element under övningen iPILOT.

Incidentrapport – bakgrund

Incidentrapport – offer



Incidentrapport – angripare

Background | Victim | Attacker | Incident descr. | Damage assessment

Node

For example the attacker's IP-address or host name. ★

User

For example the specific user carrying out the attack. ★

Comment

Any further details concerning the attacker you find relevant. ★

Incidentrapport – beskrivning

Background | Victim | Attacker | Incident descr. | Damage assessment

Suspected attack objective

- ○ Obtain system privilegies (e.g. to remotely control a machine)
- ○ Obtain information (e.g. network scans or eavesdropping)
- ○ Influence a system's functionality (e.g. denial-of-service attacks)

Attack or vulnerability details

Describe the attack, e.g. by the CVE code of the exploited vulnerability.

Attack mechanism(s) believed to be used (from CAPEC)

- ☐ Collect and Analyze Information
- ☐ Inject Unexpected Items
- ☐ Engage in Deceptive Interactions
- ☐ Manipulate Timing and State
- ☐ Abuse Existing Functionality
- ☐ Employ Probabilistic Techniques
- ☐ Subvert Access Control
- ☐ Manipulate Data Structures
- ☐ Manipulate System Resources

Attack domain(s) believed to be concernced (from CAPEC)

- ☐ Social Engineering
- ☐ Supply Chain
- ☐ Communications
- ☐ Software
- ☐ Physical Security
- ☐ Hardware

Incidentrapport – bedömd skadeverkan

Background | Victim | Attacker | Incident descr. | Damage assessment

Success probability

0-10%	11-20%	21-30%	31-40%	41-50%	51-60%	61-70%
71-80%	81-90%	91-100%				

The probability that the attackers succeeded with the attack.

Asset criticality

1	2	3	4	5	6	7

The criticality of the asset under attack.
1 is not critical and 7 is very critical.

Attack impact

1	2	3	4	5	6	7

The attack's impact on your business process(es)
1 is low impact and 7 is high impact.

Response urgency

1	2	3	4	5	6	7

The urgency to mitigate the threat.
1 is low urgency and 7 is high urgency.

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