Welcome to

6. Operate, Respond and Forensics

KEA Kompetence SIEM and Log Analysis

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg

6-operate-respond-forensics.tex in the repo security-courses

Goals for today

Todays goals:

- Operate a SIEM - further discussions how to work with the SIEM you setup
- Respond and Forensics – relating this course with incident response and forensics
- Exam preparation – Trial exam, show how it works

Photo by Chris Benson on Unsplash

Plan for today

Subjects

- Go through exam reading list, Literature list walkthrough, Subject list walkthrough

Exercises

- Find case management solutions
- Exam demo

Reading Summary

Read CIP 6 Operationalize!

Skim: SOC 9. vuln management and 10. Data Orchestration

Papers: Skim table of contents Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics, ENISA

Reading Summary, continued

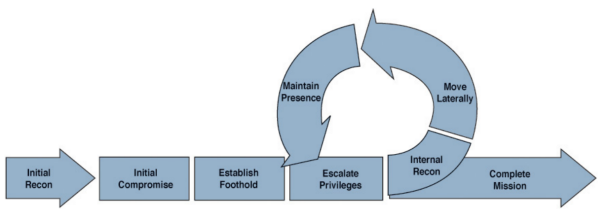


Figure 7-1 *Targeted Attack Lifecycle*

> Many breaches discovered are caused by a system having a known vulnerability exploited before it is properly patched.

Source: Mandiant's Targeted Attack Lifecycle, SOC chapter 7. vuln management

- Chapter contains lots of references
- Also chapter links inventory controls with active discovery tools and mitigating
- Mentions Threat Feeds, which should be integrated into SIEM and/or organizations
- You need to stay up-to-date on current threats, and be able to search for signs in your own network

Reading Summary, continued

Let's start by talking a little bit about events, because they might not be what you think they are.
As discussed earlier, events are really things we observe based on artifacts we have that you can use to indicate what may have happened in the recent (or in some cases, distant) past. **For most new SOCs**, this tends to mean focusing on the events that come in the form of **logs generated by assets and security controls throughout the organization, or collated events that analyze multiple logs in the context of each other**. As a result, SOC members spend a lot of time working on building and tuning security log management and **security information and event management (SIEM)** to help collect and interpret such **logs in real time or over historical periods.** Unfortunately, events in the form of automated logs or alerts generated by SIEMs represent the smaller portion of events relevant to security incidents in most organizations.

Source: SOC 11. Reacting to events and Incidents

- Elasticsearch and Logstash typically stores the original message too

Reading Summary, continued

> You will need at least one dedicated and full-time human to analyze your security event data. ... For organizations with too few dedicated security analysts, the actual available headcount may define with what frequency and what volume alerts can be handled per day or week. Ideally, organizations are staffed to run and process all defined reports, with enough flexibility for new reports to be created and analyzed.

Source: CIP 6 Operationalize!

- Organizations in Denmark does not usually have the luxury of dedicated resources – until it happens

Staffing your security team

With regard to analysts and staffing, your options essentially boil down to:

- Paying a managed security service a regular subscription fee to "do your security," with little to no context about your network; the service might, however, handle a broad spectrum of security beyond incident response (e.g., vulnerability scan- ning)
- Tasking a part-time "security person" to work on a best-effort security monitor- ing system (e.g., a SIEM) when they have time
- Hiring a sufficient number of security analysts and tailoring your security opera- tions to your business requirements
- Calling in an emergency response team after your organization has been compromised

Source: CIP 6 Operationalize!

- Hard truth

Reading Summary, continued

Papers: Skim table of contents Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics, ENISA

- When we collect data it may become sensitive
- Metadata matters – a lot!
- Forensics often use data from the SIEM and logging systems
- ENISA is the *European security office*

Goals: SIEM and Log Analysis

We have learned a lot about SIEM and Logging, in some detail

Often we can reuse existing systems, setups, examples

Elasticsearch is only one example system, but covers a lot

Photo by NESA by Makers on Unsplash

Literature list walkthrough

Our reading list is at:

https://github.com/kramse/kea-it-sikkerhed/blob/master/siem-og-loganalyse/lektionsplan.md

Not all are required reading for the exam!

We will now go through the list and comment, ask questions

Selection criteria and goals:

- You should be able to read books, presentations, papers, vulnerability disclosures, hacker zines.
- You should be able to find and use tools and frameworks
  Example MITRE ATT&CK, Elastic guides, Blog posts

A lot of resources are also linked throughout the course presentations

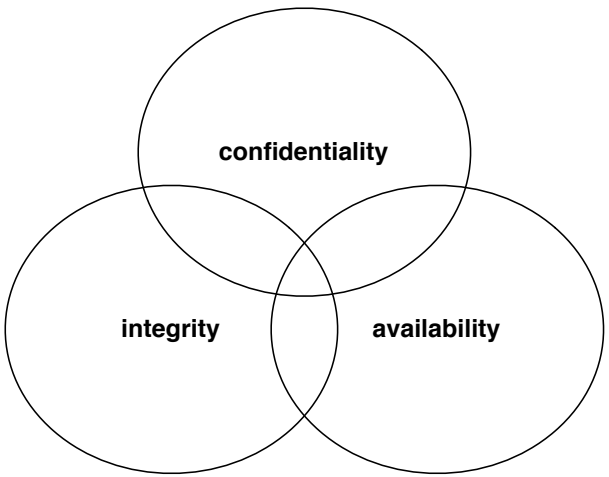
Books we worked with

Primary literature:

- *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis
  ISBN: 978-1-118-79372-5 February 2014 https://datadrivensecurity.info/ - short DDS
- *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*
  by Jeff Bollinger, Brandon Enright, and Matthew Valites ISBN: 9781491949405 - short CIP
- *Intelligence-Driven Incident Response*
  Scott Roberts ISBN: 9781491934944 - short IDI
- *Security Operations Center: Building, Operating, and Maintaining your SOC*
  ISBN: 9780134052014 Joseph Muniz - short SOC

By now we should have an idea where to find details about for example Netflow, or incident response, so we can create real systems using the methods

Confidentiality, Integrity and Availability



We want to protect something

Confidentiality - data kept a secret

Integrity - data is not subjected to unauthorized changes

Availability - data and systems are available when needed

Security is a process

Remember:

- what is information and security?
- Data kept electronically
- Data kept in physical form
- Dont forget the human element of security

Incident Response and Computer Forensics reaction to incidents

Good security is the result of planning and long-term work

Security is a process, not a product, Bruce Schneier

Source for quote: https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

Work together

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

VERIS

> Verizon RISK Team. "2013 data breach investigations report." Available at http://www.verizonenterprise.com/DBIR—This report is based on data collected using the VERIS framework. You might find it handy to look at some of the graphics in the report and then attempt to repeat them using the verisr package, discussed in this chapter, and the VCDB data.

Source: DDS page 189

Related to the Risk rating SOC chapter 7. vuln management, we often need a common format and terminology

Automated IOC Formats

Automated IOC Formats

Fully automated and comprehensive formats such as OpenIOC and STIX are useful only for teams that use tools built for them (or are capable of of building tools to use these standards).

Source: IDIR page 198

- Veris and other standardized format are a benefit
  http://veriscommunity.net/
  VERIS the vocabulary for event recording and incident sharing
- Most come from a need, but few are implemented across the industry

What are some of the yearly reports you like?

Exercise: Find 3 security reports

- The Data Breach Investigations Report from Verizon is located at: https://enterprise.verizon.com/resources/reports/dbir/
- Find three similar ones from other companies and organizations
- Use search terms like: The State of Network Security
- or companies working with security: Mandiant, Fireeye, firewall vendors
- or companies recently breached: Solarwinds
- or network organizations:

Note: a lot of them publish these around new year, so about now and January

Sample reports from ENISA

ENISA Consolidated Annual Activity Report 2023

This publication presents the annual activity report of ENISA for 2023. The report is based on the 2023 work programme as approved by the agency's Management Board.

https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2023

ENISA Threat Landscape 2023

This is the eleventh edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape. It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures. This year's work has again been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Case management

There are a number of open source and commercial case management tools available on the market, most sharing a set of common features. Most coordinate the end-to-end response, investigation, and reporting of security incidents. Most provide a secure web-based collaboration platform that allows for multiple parties to work together to investigate incident reports and manage incidents. Most provide the ability to report on individual incidents and provide trending data for longer-term analysis. Most provide some level of integration with other systems to streamline investigations and response, particularly integration with SIEMs, forensics platforms, and enterprise ticketing systems. Some also support compliance and security incidents, providing for anonymous incident reporting for ethics violations.

Source: SOC 11. Reacting to events and Incidents

Example tools

- Malware Information Sharing Platform (MISP) https://www.misp-project.org/
- *GRR Rapid Response is an incident response framework focused on remote live forensics.* https://github.com/google/grr
- *A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.* https://thehive-project.org/
- CIP book mention that: *Cisco's CSIRT uses Bugzilla as its playbook management https://www.bugzilla.org/ software*
- Collaborative Research into Threats (CRITS)
- Your Everyday Threat Intelligence (YETI)
- FIR https://github.com/certsocietegenerale/FIR – via IDIR book page 117
  FIR is an open source ticketing system built from the ground up to support intelligence-driven incident response.

Lets discuss, which ones would you try? Have you tried, how to decide, maintained software?

SIEM tools

- Alientvault OSSIM, OSSEC, Sagan, Splunk Free
- Snort, Elasticsearch, MozDef, ELK Stack, Wazuh
- Apache Metron – Apache Metron evolved from Cisco's Open SOC platform

10 Best Free and Open-Source SIEM Tools https://www.dnsstuff.com/free-siem-tools

10 Best SIEM Tools https://www.dnsstuff.com/siem-tools

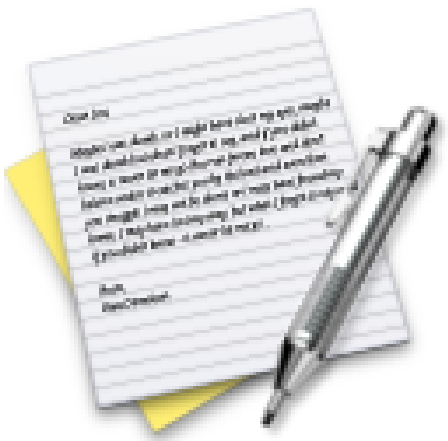
- The ELK Stack
- Apache Metron
- SIEMonster
- Prelude
- OSSIM

A lot of web pages contain the same lists of tools – and sorry, these tools are not all great at being a SIEM!

Exercise: Find case management solutions

- Use search terms like CSIRT, FIRST, Veris, MISP,

Exercise



Now lets do the exercise

ℹ Research MISP Project 45min

which is number 23 in the exercise PDF.

Exposure, Attack surfaces, and reducing them

- Incident prevention
- Real-time intrusion detection systems (IDS/IPS)
- **Definition 27-7** An *attack surface* is the set of entry points and data that attackers can u se to compromise a system.
- Reducing the chance of success also helps, randomization
- Use stack and heap protection
- Address space layout randomization (ASLR) is a host-level moving target defense.
- OpenBSD even randomizes the kernel on install – kernel address randomized link (KARL)
- Limit number of listening services, change insecure defaults, implement access control and firewalls
- Remove anything but the necessary request methods on web servers `GET`, `HEAD` and `POST`
- Restrict access to administrative interfaces
- Implement network segmentation

Subjects: Incident Response

Context, what are the threats, what are the answers we want from the SIEM and Logs

What are the common cases, where we use the data?

- Incident Response
- Computer Emergency Response Team (CERT) and Computer Security Incident Response Teams (CSIRT)
- Security Departments
- GDPR Data protection
- Computer Forensics

Detection Capabilities

Security incidents happen, but what happens. One of the actions to reduce impact of incidents are done in preparing for incidents.

> *Preparation* for an attack, establish procedures and mechanisms for detecting and responding to attacks

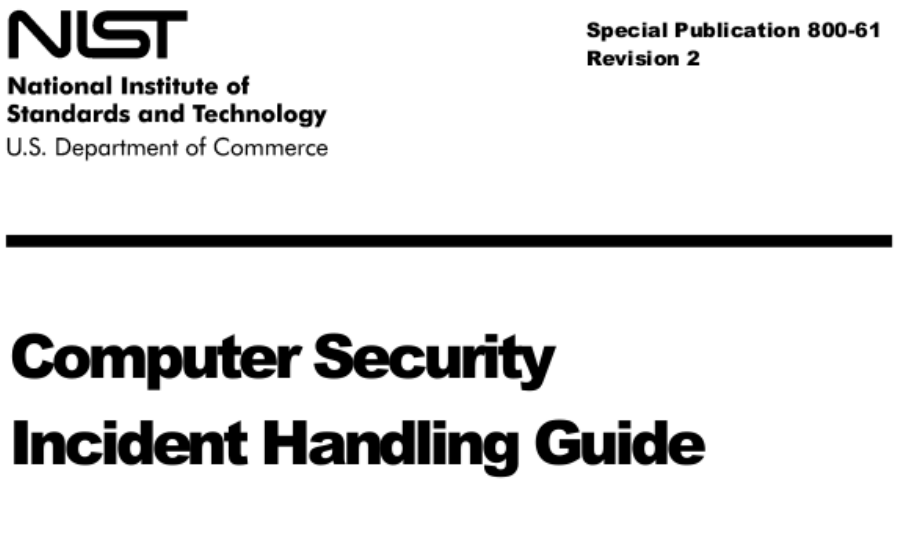
Preparation will enable easy **identification** of affected systems, better **containment** which systems are likely to be infected, **eradication** what happened – how to do the **eradication** and **recovery**.

Incident Handling, phases

The procedures developed for incident response must cover the complete life-cycle

- Preparation for an attack, establish procedures and mechanisms for detecting and responding to attacks
- Identification of an attack, notice the attack is ongoing
- Containment (confinement) of the attack, limit effects of the attack as much as possible
- Eradication of the attack, stop attacker, block further similar attacks
- Recovery from the attack, restore system to a secure state
- Follow-up to the attack, include lessons learned improve environment

Book: NIST SP800-61rev2



https://doi.org/10.6028/NIST.SP.800-61r2

Incident Response Checklists

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

This checklist is from the NIST document *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-61 Revision 2, August 2012.

Incident Response Life cycle

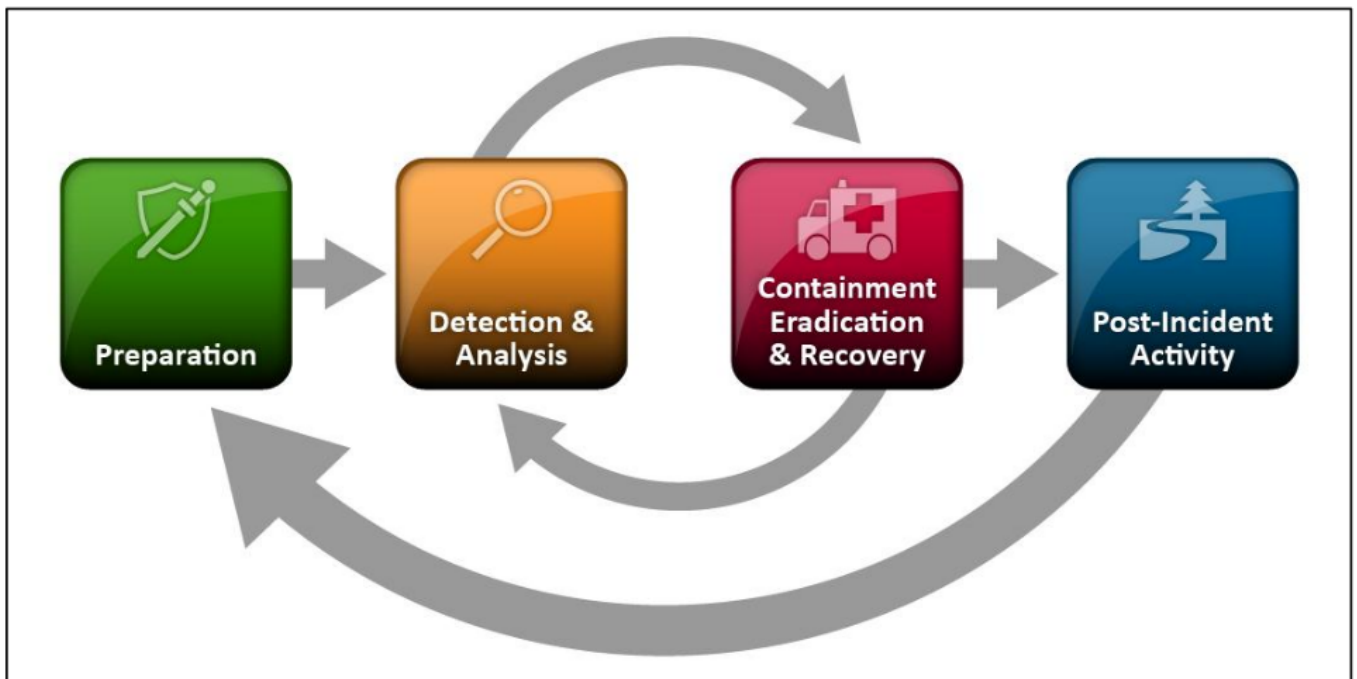


Figure 3-1. Incident Response Life Cycle

Source: *Computer Security Incident Handling Guide*, NIST SP 800-61 Rev. 2

Network Forensics ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe.

ENISA is contributing to a high level of network and information security (NIS) within the European Union, by developing and promoting a culture of NIS in society to assist in the proper functioning of the internal market.

https://www.enisa.europa.eu/

ENISA has published a number of training documents which are free to use, so these are our basics.

See more at:

https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/training-courses

Forensic analysis

> Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection 5 .

Systems used to collect network data for forensics use usually come in three forms:

- Packet capture: All packets passing through a certain traffic point are captured and written to storage
- Intrusion detection systems
- Network flow sensors

The acronym OSCAR 8 stands for: Obtain information, Strategize, Collect evidence, Analyse, Report

Source: Forensic analysis Network Incident Response Handbook, Document for teachers 1.0 DECEMBER 2016, ENISA `EXE2_Forensic_analysis_II-Handbook.pdf`

ENISA papers

- I recommend these as examples:
- ENISA Presenting, correlating and filtering various feeds Handbook, Document for teachers
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/presentin
- ENISA Forensic analysis, Network Incident Response
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-reso
  exe2_forensic_analysis_ii-handbook
- ENISA Network Forensics, Handbook, Document for teachers
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/network-

They are focussed on network forensics, which is required to do network-wide investigations. '

You also need application and client logs

Chain of custody

> Chain of custody (CoC), in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence.

Source: https://en.wikipedia.org/wiki/Chain_of_custody

- Put things in a bag, tape it closed, write what is inside, date, who collected etc.

GDPR, logging and legality

> 10.Stiller GDPR krav om logning af alt, herunder hvad den enkelte bruger laver på systemet, hvad han ser mv.?
>
> SikkerhedsBranchens opfattelse er at det er nok at logge hvem der er logget ind i systemet i hvilket tidsrum. Princippet i den gamle persondatalovs § 41 stk. 3 er ført videre i GDPR, og praksis derfra understøtter vores opfattelse.

Source:

https://www.sikkerhedsbranchen.dk/wp-content/uploads/2018/12/GDPR-Databeskyttelse-FAQ.pdf

- Most references are about GDPR and logging
- Keywords gdpr siem site:dk
- https://digst.dk/styring/standardkontrakter/klausuler-til-informationssikkerhed/logning/

Monitoring of employees

Overvågning på arbejdspladsen

På en tredjedel af IT-arbejdspladserne overvåges IT-medarbejdernes brug af e-mails og Internet. Det viser en lille stikprøveundersøgelse, som PROSA har foretaget. PROSA ønsker klare regler på området og vil derfor på en række møder være med til at sætte gang i overvågningsdebatten

Source: 2001 PROSA https://www.prosa.dk/artikel/overvaagning-paa-arbejdspladsen-1/

- Also https://www.prosa.dk/artikel/regler-for-it-overvaagning-paa-arbejdspladsen/
- If your IT-security policies allow private use of devices and systems, be careful
- Even if your IT-security policies do not allow, people might store private data
- If you need to access data, **for operational purposes**, you ARE allowed in DK
- Recommend informing employees and others specifically

Danish Data Protection Agency: Employee data

> Databeskyttelse i forbindelse med ansættelsesforhold er et komplekst område, hvor bl.a. de overordnede databeskyttelsesretlige regler, ansættelsesretlige regler samt kollektive overenskomster og aftaler har betydning for de behandlinger af personoplysninger, der sker på arbejdspladser og i fagforeninger, mv.
>
> Såvel offentlige som private arbejdsgivere behandler en stor mængde personoplysninger om ansøgere i forbindelse med rekruttering og om medarbejdere, både under ansættelsen og efter ansættelsens ophør. Tilsvarende behandler faglige organisationer og tillidsrepræsentanter personoplysninger om både deres medlemmer og andre medarbejdere på arbejdspladsen. Hertil kommer, at der i vidt omfang udveksles oplysninger mellem de enkelte aktører.

Source: https://www.datatilsynet.dk/media/7597/databeskyttelse-i-forbindelse-med-ansaettelsesforhold.pdf

- Probably one of the best sources to use, as they process complaints about data processing
- 43 pages

Exam preparation

Afgangsprojektet (15 ECTS)	
Der udvikles løbende nye valgfag til Diplom i it-sikkerhed. Disse vil løbende blive beskrevet i en allonge (bilag 2) til studieordningen.	
Sikkerhed i it-governance (it-sikkerhedsledelse) (5 ECTS)	Softwaresikkerhed (10 ECTS)
Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)	
Systemsikkerhed (10 ECTS)	
Netværks- og kommunikationssikkerhed (10 ECTS)	

Overview Diploma in IT-security

Deliverables and Exam

- Exam
- Individual: Oral based on curriculum
- Graded (7 scale)
- Draw a question with no preparation. Question covers a topic
- Try to discuss the topic, and use practical examples
- Exam is 30 minutes in total, including pulling the question and grading
- Count on being able to present talk for about 10 minutes
- Prepare material (keywords, examples, exercises, wireshark captures) for different topics so that you can use it to help you at the exam

- Deliverables:
- 1 Mandatory assignments
- Mandatory assignments are required in order to be entitled to the exam.

Course Description

From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018
VF4 SIEM og log analyse (5 ECTS)

Indhold
Den studerende lærer om Security information and event management (SIEM), herunder hvordan man kan indsamle, administrere, og søge i sikkerhedshændelsesdata i et større it system (komplekse systemer, IOT deployments, corporate IT).

Læringsmål
Viden – Den studerende har viden om og forståelse for:

- Typiske SIEM arkitekturer
- Standard logformater og logtyper for standard systemer og komponenter
- Typiske SIEM produkter
- Juridiske krav til logning og bevarelse af data ifb. forensic analyse

Færdigheder – Den studerende kan:

- Lave en baseline-analyse af en infrastruktur
- Bruge log-data til at identificere infrastrukturkomponenter
- Bruge et værktøj til at analysere system log-data og netværkstrafik til at finde sikkerhedshændelser
- Udvikle "dashboards"og alarmer der viser tegn på hændelser

Kompetencer – Den studerende kan:

- Designe og implementere en SIEM løsning på tværs af diverse produkter
- Træffe beslutninger om hvilke data der skal indsamles i en givne situation
- Identificerer fejl i logopsamlingen
- Deltage i drøftelser på et praktisk og strategisk niveau i forhold til implementering af logmanagement/SIEM

Final word is the Studieordning which can be downloaded from

https://kompetence.kea.dk/uddannelser/it-digitalt/diplom-i-it-sikkerhed

Studieordning_for_Diplomuddannelsen_i_IT-sikkerhed_Aug_2018.pdf

Mundtlig eksamen og formalia

Eksamen varer samlet set i 30 minutter og forløber i 4 faser:

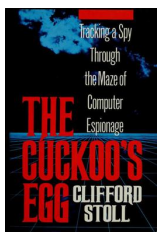
1. Du trækker indledningsvist ét af de 10 ovenstående emner
2. Du forklarer indledende emnet støttet af egne slides i op til 10 minutter
3. Herefter uddyber og diskuteres emnet i en dialog på 10 – 15 minutter
4. Afslutningsvist er der 5 minutters votering og karaktergivning

Karakteren vil være en helhedsbedømmelseaf din viden om emnet samt din evne til at uddybe og diskutere relevante IT-sikkerhedsmæssige elementer. Der gives karakter efter 7 trins skalaen.

Exam subjects, with keywords

- **1) Overview of SIEM** The SIEM name, dive into events - common data used/found in events SOC, IOC and other acronyms that are found in this course
- **2) Data types** IP address, domain names and DNS, reputation lists, formats JSON, XML, CSV ISO8601 - normalization Netflow and TCP/IP, AS numbers, CIDR, port numbers
- **3) Tools used in the SIEM world** Languages, Zeek, Python, cURL, JavaScript, CSS, R Any tools you like, really
- **4) Storing and processing data – log data in particular** Elastic stack, Logstash - ingestion and normalization, ES store/process, Kibana present REST, Message queuing Filebeat, packetbeat
- **5) Dashboards and visualization of event data** process of using, searching in data Elasticsearch Elastic Common Scheme (ECS) Elasticsearch SIEM How standard schemes help
- **6) SIEM architectures** Present some sample architectures, use some of the tools presented like HELK and Elastic stack overviews Explain some problems - scalability, how to cope with lots of data

Afterword



> **Threat intelligence was vital to intrusions over 20 years ago**, starting with the story told in **the Cuckoo's Egg, written by Cliff Stoll**, and has been ever since. But somehow, most organizations are **still learning** to adopt the same principles. ... Lucky for us, this book now exists and steps the reader through **proper threat-intelligence concepts, strategy, and capabilities** that an organization can adopt to evolve their security practice. After reading this book, your operations can grow to become an intelligence-driven operation that is much more efficient than ever in **detecting and reducing the possible impact of breaches that will occur.**

Source: Foreword in *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown