



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@Github 

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

# Goals for today



Todays goals:

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

Photo by Chris Benson on Unsplash

# Plan for today



## Subjects

- 3 slides from last time: Reporting/Automatic reporting: tcpflow
- Go through exam reading list, Literature list walkthrough, Subject list walkthrough

## Exercises

- Exam demo
- Find State of security and breach reports
- Find case management solutions

## Reading Summary



SOC 7. vuln management

SOC 11. Reacting to events and Incidents

CIP 6 Operationalize!

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

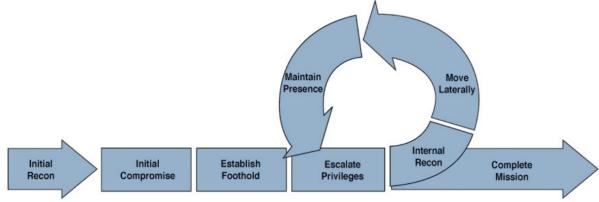


Figure 7-1 Targeted Attack Lifecycle

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 scanning)
- Tasking a part-time “security person” to work on a best-effort security monitoring system (e.g., a SIEM) when they have time
- Hiring a sufficient number of security analysts and tailoring your security operations 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://zencurity.gitbook.io/kea-it-sikkerhed/siem-and-log-analysis/lektionsplan>

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

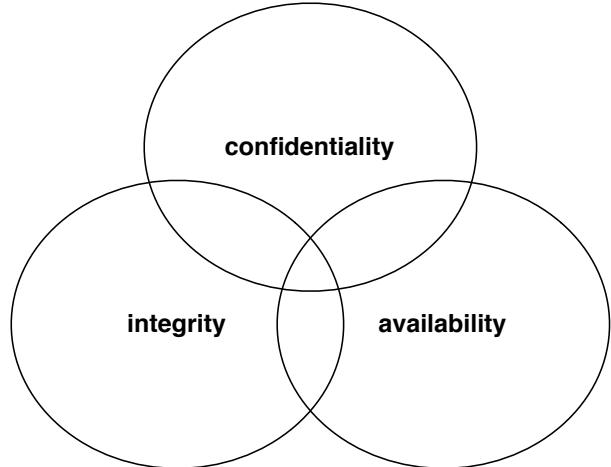


Primary literature:

- *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](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

# 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)	Systemsikkerhed (10 ECTS)
Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)	
Softwaresikkerhed (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 arkitekturen
- 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 diskutes emnet i en dialog på 10 – 15 minutter
4. Afslutningsvist er der 5 minutters votering og karaktergivning

Karakteren vil være en helhedsbedømmelse af 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 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



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 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:

Example: ENISA *Trust Services Security Incidents 2019 Annual Analysis Report*

<https://www.enisa.europa.eu/publications/trust-services-security-incidents-2019-annual-analysis-report> Note: a lot of them publish these around new year, so about now and January

## 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

- <https://www.misp-project.org/>
- Request Tracker for Incident Response (RTIR) <https://bestpractical.com/rtir/> mentioned in the SOC book, but not sure I would recommend RT anymore
- *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

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

## SIEM tools



- Alienvault 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>

# SIEM tools



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

A lot of web pages contain the same lists of tools

Comparison, almost random link – a SIEM vendor:

*7 Open Source SIEMs: Features vs. Limitations*

<https://www.exabeam.com/siem/7-open-source-siems-features-vs-limitations/>

## Exercise: Find case management solutions



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

# 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 use 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

## 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 network forensics documents which are free to use, so these are our basics.

# 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...](https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/presenting)
- 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](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/overvaagningspaaarbejdspladsen-1/>

- Also <https://www.prosa.dk/artikel/regler-for-it-overvagning-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