Welcome to

6. Reporting on Incident Response

Introduction to Incident Response Elective, KEA

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Codeberg https://codeberg.org/kramse/
6-Reporting-on-Incident-Response.tex in the repo security-courses

Goals for today

- Connect knowledge from previous days
- Do a big exercise using knowledge from the class so far
- Prepare you to work as incident responders in the future
- Collect a playbook – get started building your own playbook

Photo by Thomas Galler on Unsplash

Plan for today

- Start out with some cases
- Get you started planning incident response
- List organizational requirements
- List preparational steps
- List specific tools you want to have, know of, buy, gather, ...

Exercise theme:

- Building your own playbook

Time schedule

This day we will be doing a larger project, get started planning incident response

- 1) Going over a few cases from Denmark – first 45min
- 2) Plan your incident response, the mission – 45 min
- Break 15min
- 3) Plan your incident response, tools – 45min
- 4) Plan your incident response, processes 45min

Times are suggested, in real life this process would take months!

Part 1: Go over a few more cases

Let's go over some of the recent cases from Denmark and internationally

You are most likely to find jobs in Denmark, and we know danish companies better

Example cases and Categories from Denmark

Start by finding a few cases from Denmark, we already talked about Maersk but feel free to re-use this data.

Cases I know are: Forsvaret (2023), Demant (2019), Ecco (2022), kommuner, infrastruktur

Try to put them in categories and find examples of each category:

- DDoS
- Data leaks – check datatilsynets perhaps
- Ransomware Demant – ransomware, but may stealing data too?
- ... more categories here, maybe use Mitre ATT&CK for inspiration

Learning from others Incident Response cases

- What did they do, consider advice from book
- Could they have responded differently
- What were they missing, could they learn from this
- What are some things we definitely would have *ready* for handling incidents
- What did it cost them, input for security budgets

Part 2-4) Plan your incident response

Congratulations – you are now the CISO

And we would like to A) Avoid incidents B) Resolve any incident efficiently

- Rest of today we will plan our incident response in Company XYX
- Essentially this will be the start of a playbook

Company XYX

This medium sized company with 100 employees produce a cheese cutter and sell them all over the world. They are the number one brand of cheese cutters, loved by chefs around the world.

- Turnover is in the millions
- Orders are flowing in through a web shop for customers
- Another web shop is used by B2B segment for ordering 1.000s of cheese cutters

Help them, they don't have a CISO, they don't have security people, they are afraid of security incidents – but don't know anything about them

Your Goal

There will be a management and board meeting soon, and you will present

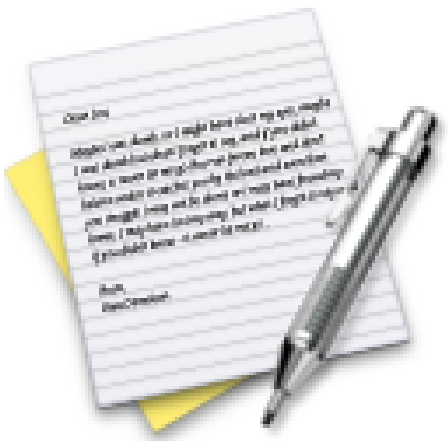
- The XYX Security Organisation
- The XYX security org mission statement
- The Basic XYX Incident Response Process
- The contact list for incident handling, feel free to add external companies
- A list of systems and tools to put in place before incidents (CMDB?)
- A list of programs, applications, tools, hardware to use for incidents (external drives and go-bag?)

Where to find inspiration

We have our main book, and have links to other documents, so feel free to find inspiration in:

- NIST documents SP800 series – NIST SP800-61r2
- Awesome lists, like: https://github.com/meirwah/awesome-incident-response

Exercise

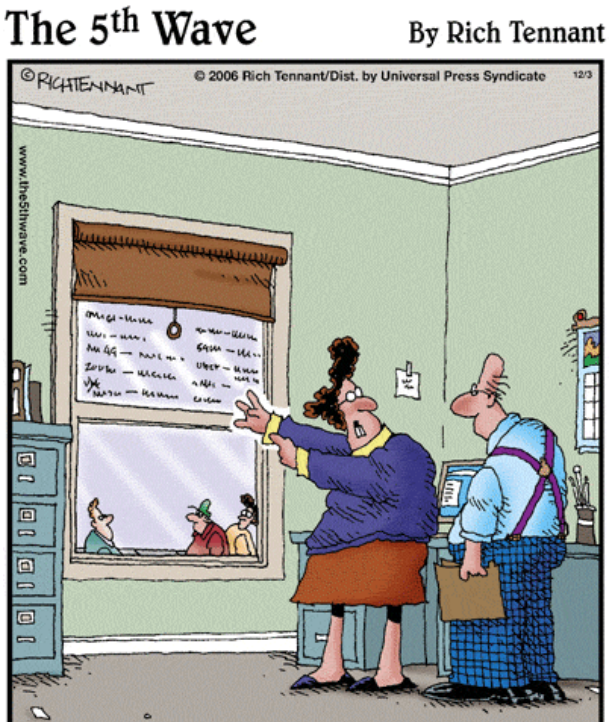


Now lets do the exercise

⚠ The Incident Response Mission 15 min

which is number **24** in the exercise PDF.

Further inspiration on the next slides



"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

Tools and Resources

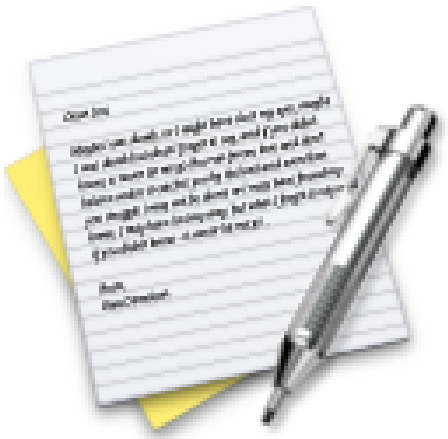
kea

You can find lots of information about tools from books, and lists on the internet.

Many things are marked with forensics – and can be used during incident response.

- Awesome lists, like: https://github.com/meirwah/awesome-incident-response
- Sigma is another popular format: for more information see *Generic Signature Format for SIEM Systems* https://github.com/SigmaHQ/sigma

Exercise



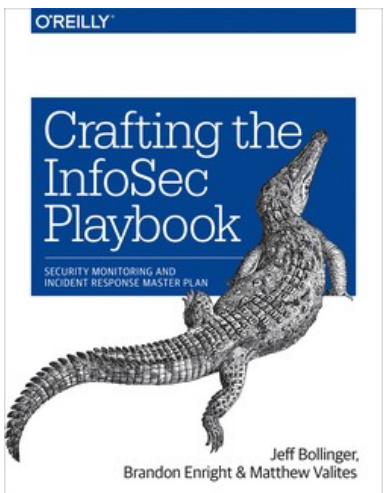
Now lets do the exercise

⚠ Create a list of *tools* 30 min

which is number **25** in the exercise PDF.

You can use https://pad.tyk.nu/

Crafting the InfoSec Playbook



Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan
by Jeff Bollinger, Brandon Enright, and Matthew Valites ISBN: 9781491949405 - short CIP

Develop your own threat intelligenceand incident detection strategy We don't have this book, but will use a checklist from the next slide.

Crafting the InfoSec Playbook

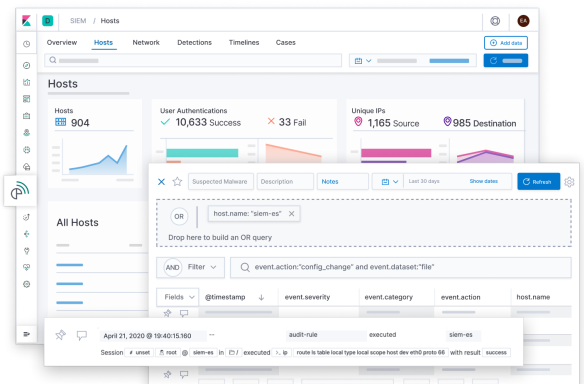
kea

This book will help you to answer common questions:

- How do I find bad actors on my network?
- How do I find persistent attackers?
- How can I deal with the pervasive malware threat?
- How do I detect system compromises?
- How do I find an owner or responsible parties for systems under my protection?
- How can I practically use and develop threat intelligence?
- How can I possibly manage all my log data from all my systems?
- How will I benefit from increased logging—and not drown in all the noise?
- How can I use metadata for detection?

Source: *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan* by Jeff Bollinger, Brandon Enright, and Matthew Valites ISBN: 9781491949405

Why Elasticsearch



Screenshot from https://www.elastic.co/siem

Recommend building a proof-of-concept infrastructure using the Elastic stack and gather experience with logging. This can be done without a license fee and the organization can then see what works and doesn't. Then using the experiences as input an informed decision can be made, to continue with this as a home grown logging and auditing solution, or buy a premade one.

SIEM

Security information and event management (SIEM) is a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes.[1]

The term and the initialism SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.[2]

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

- Note: there are alerting examples towards the bottom of the page, with sources
- Closely related to log management, incident response

SOC

> An information security operations center (ISOC or SOC) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.
>
> ...
>
> A security operations center (SOC) can also be called a security defense center (SDC), security analytics center (SAC), network security operations center (NSOC),[3] security intelligence center, cyber security center, threat defense center, security intelligence and operations center (SIOC). In the Canadian Federal Government the term, infrastructure protection center (IPC), is used to describe a SOC.

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

- We have a whole book about SOCs, but I skipped the introductory chapters!
- If you need to build a SOC, that is great source of information

Baseline Skills

- Threat-Centric Security, NSM, and the NSM Cycle
- TCP/IP Protocols
- Common Application Layer Protocols
- Packet Analysis
- Windows Architecture
- Linux Architecture
- Basic Data Parsing (BASH, Grep, SED, AWK, etc)
- IDS Usage (Snort, Suricata, etc.)
- Indicators of Compromise and IDS Signature Tuning
- Open Source Intelligence Gathering
- Basic Analytic Diagnostic Methods
- Basic Malware Analysis

Source: *Applied Network Security Monitoring Collection, Detection, and Analysis*, Chris Sanders and Jason Smith

Strategy for implementing identification and detection

We recommend that the following strategy is used for implementing identification and detection.

We have the following recommendations and actions points for logging:

- ☐ Enable system logging from servers
- ☐ Enable system logging from network devices
- ☐ Centralize logging
- ☐ Add search facilities and dashboards
- ☐ Perform system audits manually or automatically
- ☐ Setup notification and notification procedures

Extended Sources

When a basic logging infrastructure is setup, it can be expanded to increase coverage, by adding more sources:

- DNS query logging – will enable multiple cases to be resolved, example malware identification and tracing, when was a malware domain queried, when was the first infection
- Session data from Firewalls, Netflow – traffic patterns can be investigated and both attacks and cases like exfiltration can likely be seen

Hint: Take the sources available first, make a proof-of-concept, expand coverage

Data Analysis Skills

Although we could spend an entire book creating an exhaustive list of skills needed to be a good security data scientist, this chapter covers the following skills/domains that a data scientist will benefit from knowing within information security:

- Domain expertise—Setting and maintaining a purpose to the analysis
- Data management—Being able to prepare, store, and maintain data
- Programming—The glue that connects data to analysis
- Statistics—To learn from the data
- Visualization—Communicating the results effectively

It might be easy to label any one of these skills as the most important, but in reality, the whole is greater than the sum of its parts. Each of these contributes a significant and important piece to the workings of security data science.

Source: *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis
ISBN: 978-1-118-79372-5 February 2014 https://datadrivensecurity.info/ - short DDS

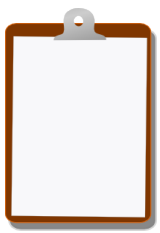
Exercise

Now lets do the exercise

⚠ Create a skills list 45 min

which is number **26** in the exercise PDF.

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools