Welcome to

8. The Way Forward: Building an Intelligence Program

Introduction to Incident Response Elective, KEA

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

Slides are available as PDF, kramse@Github

8-The-Way-Forward-Building-IR-Program.tex in the repo security-courses

Goals for today

- Talk about the big picture
- Strategic Intelligence
- Summary of the course

Photo by Thomas Galler on Unsplash

Plan for today

- Go through last chapters from the book
- Strategic Intelligence
- Building an Intelligence Program – prepare you to implement incident response
- Exam subjects, questions, finishing up

Exercise theme:

- Revisit some exercises? especially if related to incident response

Time schedule

- 1) Chapter 10: Strategic Intelligence – 45min
- 2) Chapter 11: Building an Intelligence Program – 45 min
- Break 15min
- 3) Exam related items – 45min
- 4) Summary and finishing up – 45min

Reading Summary

Intelligence-Driven Incident Response (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781491934944

- Chapter 10: Strategic Intelligence
- Chapter 11: Building an Intelligence Program

The Way Forward

Intelligence-Driven Incident Response (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781491934944

> Intelligence-driven incident response doesn't end when the final incident report has been delivered; it will become a part of your overall security process. Part 3 covers big-picture aspects of IDIR that are outside individual incident-response investigations. These features include strategic intelligence to continually learn and improve processes, as well as implementation of an intelligence team to support security operations as a whole.

- What do you know about the *overall security process*?
- How does this subject incident response fit in?

Chapter 10: Strategic Intelligence

> Every once in while, an incident responder will start an investigation with a prickling sensation in the back of his mind. Some call it a premonition, some call it deja vu, but as the investigation unwinds, it will inevitably hit him: he has done this before. This. Exact. Same. Investigation.

Source: *Intelligence-Driven Incident Response* (IDIR)

- Putting out fires takes time, but sometimes you should let the current fire burn, and work on things to prevent and catch future fires

What Is Strategic Intelligence?

> Strategic intelligence gets its name not only from the subjects that it covers, typically a **high-level analysis of information with long-term implications**, but also from its audience. **Strategic intelligence is geared toward decision makers** with the ability and authority to act, because this type of intelligence should shape policies and strategies moving forward. This doesn't mean, however, that leadership is the only group that can benefit from these insights. Strategic intelligence is **extremely useful to all levels of personnel** because it can help them understand the surrounding context of the issues that they deal with at their levels.

Source: *Intelligence-Driven Incident Response* (IDIR)

- Understanding and working together makes a difference

The State of Strategic Analysis

> In his paper, "The State of Strategic Analysis," John Heidenrich wrote that "a strategy is not really a plan but the logic driving a plan." When that logic is present and clearly communicated, analysts can approach problems in a way that supports the overarching goals behind a strategic effort rather than treating each individual situation as its own entity.

Source: *The State of Strategic Analysis* John Heidenrich via *Intelligence-Driven Incident Response* (IDIR)

- Many companies in Denmark does NOT have a clear strategic plan, mission or ideas of how to *do security*
- Most companies in Denmark consider security an after-thought, burden, cost, annoying
- Various organisations have tried to do *maturity models* for software and security

CIS Controls: Incident Response

CIS Critical Security Control 17: Incident Response and Management

Overview

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Source: https://www.cisecurity.org/controls/incident-response-management

Developing Target Models

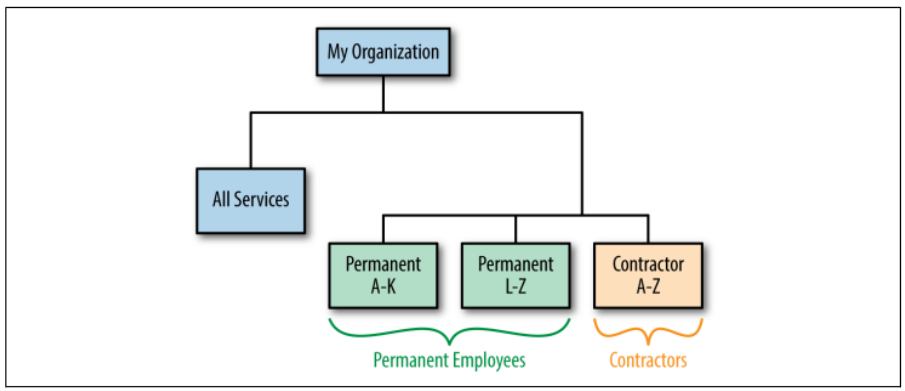


Figure 10-1. Hierarchical model

Hierarchical models are traditionally used to show personnel or roles, but one unique application of a hierarchical model is to use it to **identify the data that is important to an organization**. A hierarchical model for data includes the broad categories of data, such as financial information, customer information, and sensitive company information.

Source: *Intelligence-Driven Incident Response* (IDIR)

Network Models

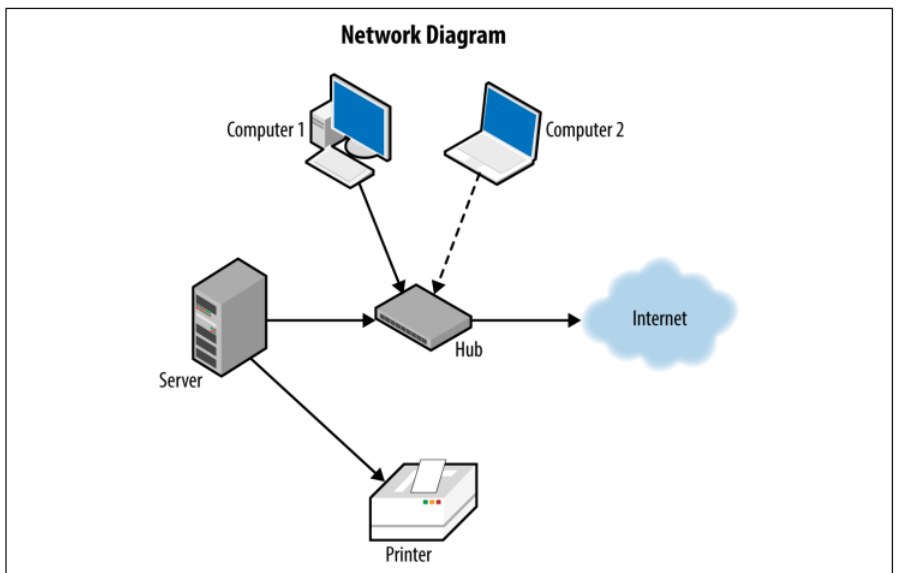
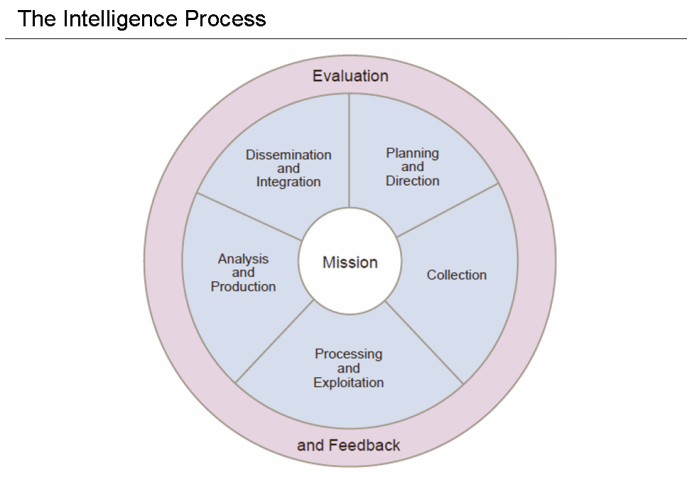


Figure 10-2. Network model example

- Process models
- Timelines – various uses, tool re-use, spread of attack types, etc.

Intelligence Cycle or Intelligence Process



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

- Chapter 10 continues applying the Intelligence Cycle/Process to the strategic level
  – which we consider high-level for now, we won't be allowed to this in most Danish companies

Conclusion

We consider strategic intelligence to be the **logic behind the plan**, and it is no wonder that many incident responders **struggle with finding the time** to conduct this level of analysis. In many organizations, incident responders would be hard-pressed to find a plan at all, much less understand the logic behind the plan. **Strategic intelligence**, when **properly analyzed and adopted by leadership**, can not only inform leadership of the long-term threats to an organization, but can also provide incident responders with policies and procedures that will **support their ability to meet the needs of their organization**.

Source: *Intelligence-Driven Incident Response* (IDIR)

- May be hard to convince leadership, so take numbers, collect data, present data
- ... or leave the organisation

Working with an **intelligence team** can be a game changer for many security operations programs. However, there needs to be **system in place** to get **everyone** on the same page, both within the intelligence team and with the customers that the team will be supporting. A **structured intelligence program** will provide the **benefit of a robust intelligence support capability** while avoiding many of the struggles teams go through when they are thrown together rather than purposely built.

- Having team members also help when handling incidents over multiple days/weeks

Are You Ready?

One question that frequently gets asked is, **"What are the prerequisites for forming an intelligence team?"** Many things need to be done before a formalized intelligence function will be beneficial. We are **not** of the mindset that an **intelligence program is the last thing** that should be created at an organization, but we do view the intelligence function as the **glue that holds many other security functions together**. If you do not have those existing functions, you will just end up standing around, holding a bottle of glue.

- Is the organisation mature enough

Questions to ask

At the far end of the spectrum of determining budget is the answer, “We were just horribly hacked and now we have to show what we are doing differently ASAP so that it never happens again. Go buy things.

Here are some fundamental questions to ask before beginning to develop an intelli- gence program, which will require funding, time, and effort:

- Is there a security function at the organization?
- Is there network visibility?
- Are there multiple teams or functions to support?
- Is there room in the budget?

Source: *Intelligence-Driven Incident Response* (IDIR)

Planning the Program

Three types of planning go into the development of a solid program: conceptual planning, functional planning, and detailed planning:

- 1. Conceptual planning sets the framework that the program should work within. Stakeholders contribute the most to conceptual planning, but it is important for them to understand what intelligence can offer them, especially if they are unfamiliar with intelligence work.
- 2. Functional planning involves input from both stakeholders and intelligence professionals to identify requirements to complete goals, logistics such as budget and staffing needs, constraints, dependencies, and any legal concerns. Functional planning provides structure and realism to the sometimes abstract conceptual planning phase.
- 3. Detailed planning is then conducted by the intelligence team, which will determine how the goals identified by the stakeholders will be met within the func- tional limits.

  All three phases of planning are important to ensure that all aspects have been considered, from budgeting to the metrics that will be reported to stakeholders.

Source: *Intelligence-Driven Incident Response* (IDIR)

Defining Stakeholders, Goals and Success Criteria

Here are a few common stakeholders:

- Intelligence response team
- Security operations center/team
- Vulnerability management teams
- Chief information security officers
- End users – are most often an indirect stakeholder for intelligence

...

After stakeholders have been defined, it is time to identify the goals of the program with respect to each stakeholder.

...

Defining concrete goals gets the stakeholders and the intelligence team on the same page by using the same definition of *success*.

Source: *Intelligence-Driven Incident Response* (IDIR)

Identifying Requirements and Constraints

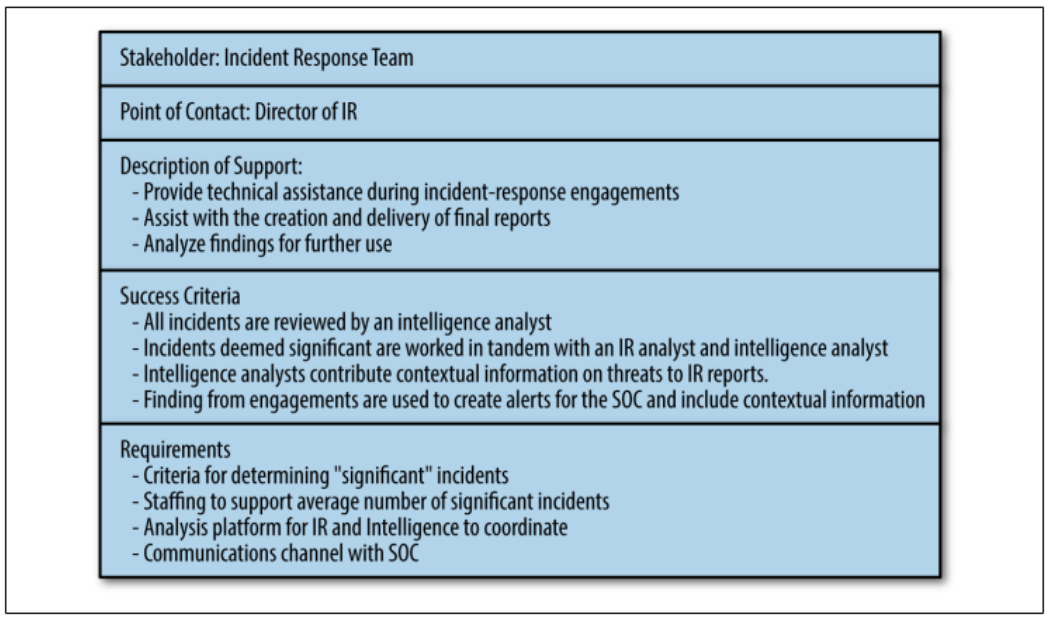


Figure 11-2. Advanced stakeholder documentation

- Probably this should be in a wiki or similar dynamic document
- Multiple organisations maintain *service documentation*

Tactical Use Cases

Tactical use cases involve intelligence that is useful on a day-to-day basis. This type of intelligence will change rapidly but can also be some of the most directly applicable intelligence in a security program.

- SOC Support: Alerting and signature development, Triage, Situational awareness
- Indicator Management: Threat-intelligence platform management, Updating indicators, Third-party intelligence and feeds management

Operational Use Cases

Operational use cases for an intelligence program **focus on understanding campaigns and trends in attacks**, either against your **own organization** or against other organizations **similar to yours**. The **sooner** a campaign can be identified or a series of intrusions tied together, the **more likely** it is that the activity can be **identified before** the attackers are **successful** in achieving their goals.

- Campaign Tracking
- Identify the campaign focus
- Identifying tools and tactics
- Response support

Strategic Use Cases

Architecture Support

Strategic intelligence can provide information not only on the ways an organization should respond to intrusions or attacks, but also on the ways it can posture itself to minimize attack surface and better detect these attacks.

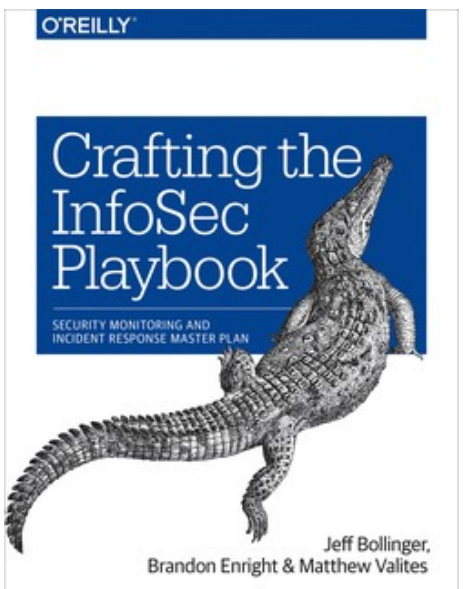
- Improve defensibility
- Focus defenses on threats

Risk Assessment/Strategic Situational Awareness

- Identify when risk changes
- Identify mitigations

Crafting the InfoSec Playbook

Maybe as a reference look into the book I suggested



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

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

Don't forget the appendix!

Book has some nice templates:

Here are some example products based on the GLASS WIZARD threat. Short-Form Products

- IOC Report: Hydraq Indicators
- Event Summary Report: GLASS WIZARD Spear Phishing Email— Resume Campaign
- Target Package: GLASS WIZARD
- Requests for Intelligence: GLASS WIZARD
- GLASS WIZARD RFI Response

Long-Form Products: Hikit Malware

Part 3: Exam related items

kea

You can now ask questions, or we can walk through all the subjects

Notes: Exam subjects for Introduction to Incident Response

- Exam will be up to 25 min
- Keywords listed are *ideas* for things to go through not a checklist
  Consider it example items that fit into this subject.
- You will only have 10 min to go through your presentation
- Feel free to include tools and references to tools throughout!
- Watch out if you do a demo! Better to have a video without audio, and talk over it
- After this we will do up to 15 min of questions and dialogue in the subject and the course

Subjects 1-2

1. Overview of Incident Response

Why do we need Incident Response, a few threats and context
Definitions of Incident Response, Computer Forensics
Main resources we have used, IDIR book, NIST, other books

2. Cyber Attack Phases and IR

Main processes and methods, intrusion kill chain, incident response cycle
Overall description of how attacks happen, and how we deal with them
Mitre ATT&CK framework can be used here

Subjects 3-4

3. Incident Response Life Cycle

Detailed about what happens when we have identified an incident
Go through the phases and explain as much as possible within 10minutes
Use NIST SP800-61r2 figure 3-1, IDIR or other books or references as you wish
You can also use the F3EAD process
You can even present overview and compare instead

4. Order of Volatility and Tools

Explain the concept of Order of Volatility (OOV) from Forensics Discovery, Farmer Venema 200
List example tools, explain how they fit with volatility
Why do we run memory tools first, and can wait with disk and storage analysis
Live Response vs cold images and files with data

kea

5. Evidence and IoCs

Anything related to facts we find and use
Definitions of IoCs, examples of IoCs
Domains, DNS, Passive DNS,
File related, Hash values, IP addresses
Enrichment and metadata related to facts
Processing of facts, where do we find them
Ideas Whois, RIPE Stat, RIPE delegated list of IP prefixes etc.
Logging can also be used here

6. Tools we have used during the course

Take your favourite tool we have used in classe, create screenshot
Walk us through the process, what it provides, how the tool helps, what is the output
Beware you CAN do demos, but if something goes wrong ... better to have a video without sound and present IMHO
Brim, tcpdump, wireshark, Packetbeat
Sysinternals
Zeek, Suricata
Volatility framework
Loki IOC and YARA scanner
MISP Project
... anything we mentioned in class or tried is OK

7. How to establish an Incident Response Capability

What are the steps to create this capability in an organisation
Use input from NIST document and IDIR book also provides detailed information
Also the exercise from March 30 may help
Select the parts of this which interest you the most, can be organizational, technical or a
Outline steps which you would propose to a CEO when you got hired as CISO

8. Vulnerability Cases

Ideas

a) Take a known vulnerability, like Log4Shell Go through how it works, what it does, what are prerequsites etc. What are some IoCs, signs of intrusion with this Focus on how this relates to Incident Response, how would an organisation react

OR

b) What preperative steps could help CMDB?, how would architecture changes reduce likelihood or prevent this from happening How can organisations learn from cases in other organisations

OR

c) Budgets and incident response Talk about steps from the incident response life cycle and how it relates to cost - usually it is MUCH more efficient to spend a little on preparation, to shorten incidents

Part 4: Finishing up in this course

I would like to use some time to finish up this course.

- Was it useful?
- Do you want to work within this specific area
- Do you want to know *about* security or work *in security*