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@Codeberg https://codeberg.org/kramse/ 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 book

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

Exercise theme:

- Revisit some exercises

Time schedule

- 1) Chapter 10: Strategic Intelligence – 45min
- 2) Chapter 11: Building an Intelligence Program – 45 min
- Break 15min
- 3) Summary and finishing up the IDIR book – 45min
- 4) Go through the NIST SP800-61r2 – 45min

Reading Summary

Intelligence-Driven Incident Response (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

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

The Way Forward

Intelligence-Driven Incident Response (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

> 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

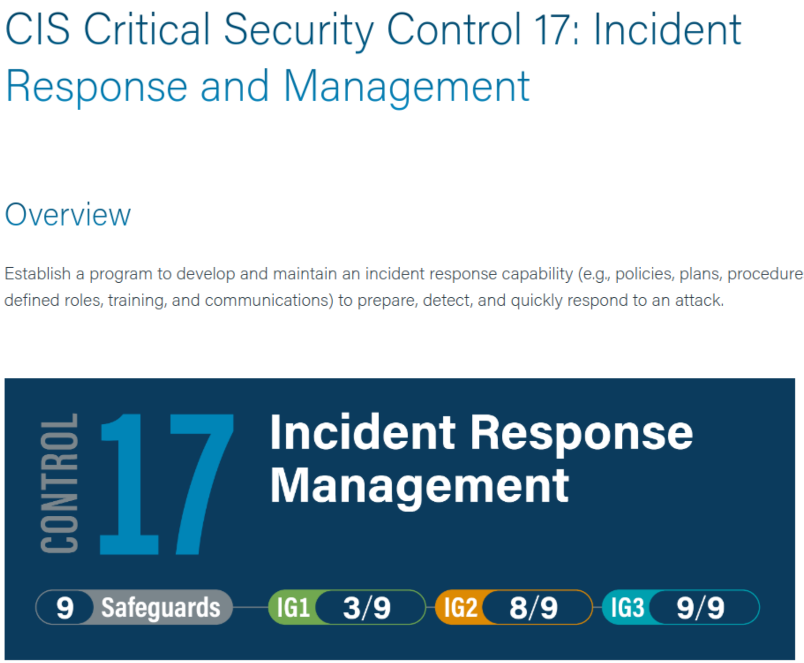
The State of Strategic Analysis

> 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

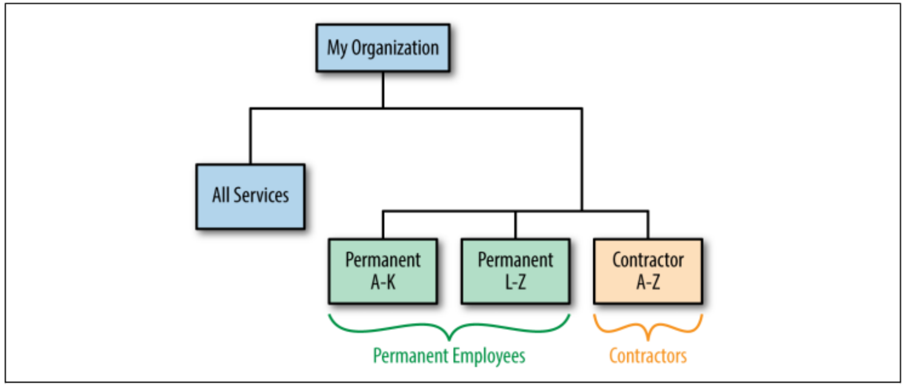


Figure 10-1. Hierarchical model

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

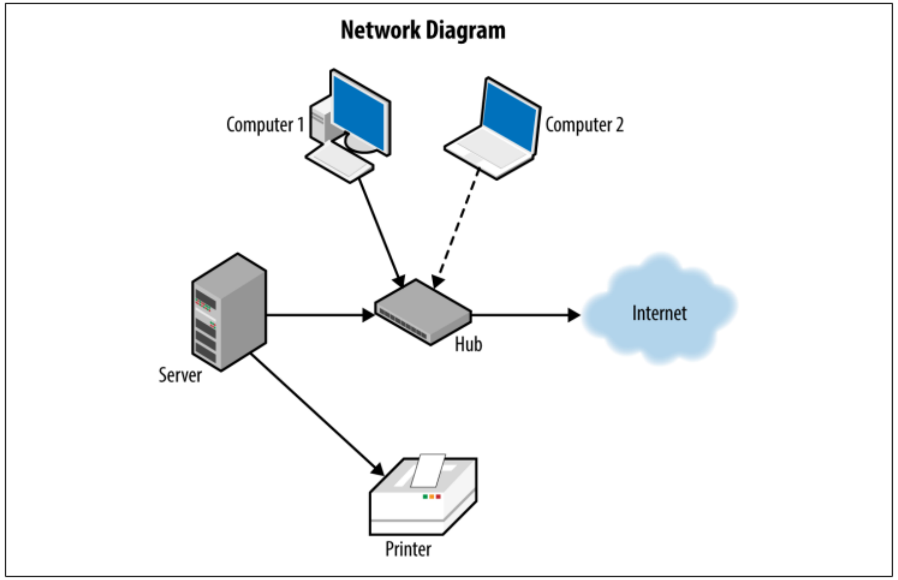
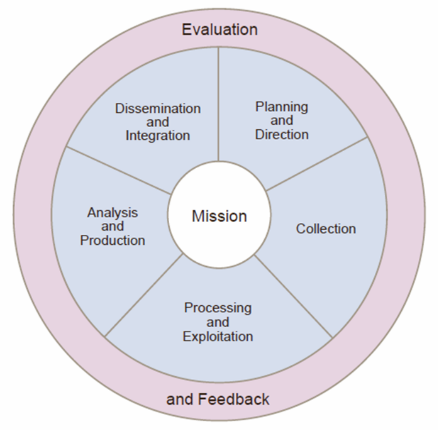


Figure 10-2. Network model example

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

Intelligence Cycle or Intelligence Process

The Intelligence Process



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

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 Strategic Intelligence

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

Chapter 11: Building an Intelligence Program

> 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

...

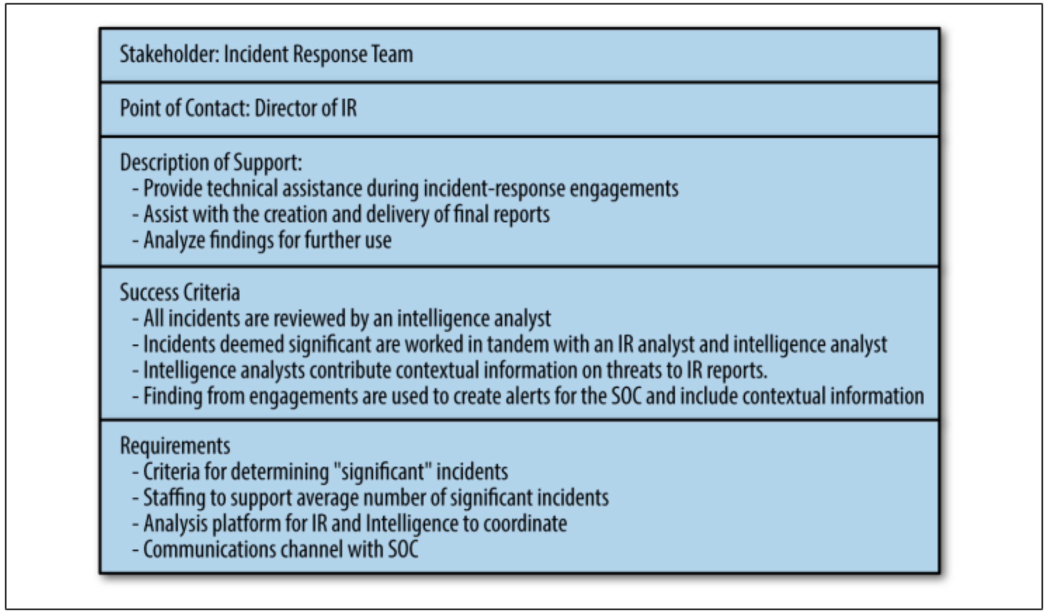
After stakeholders have been defined, it is time to identify the goals of the program with respect to each stakeholder.

...

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



Stakeholder: Incident Response Team

Point of Contact: Director of IR

Description of Support:
- Provide technical assistance during incident-response engagements
- Assist with the creation and delivery of final reports
- Analyze findings for further use

Success Criteria
- All incidents are reviewed by an intelligence analyst
- Incidents deemed significant are worked in tandem with an IR analyst and intelligence analyst
- Intelligence analysts contribute contextual information on threats to IR reports.
- Finding from engagements are used to create alerts for the SOC and include contextual information

Requirements
- Criteria for determining "significant" incidents
- Staffing to support average number of significant incidents
- Analysis platform for IR and Intelligence to coordinate
- Communications channel with SOC

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.

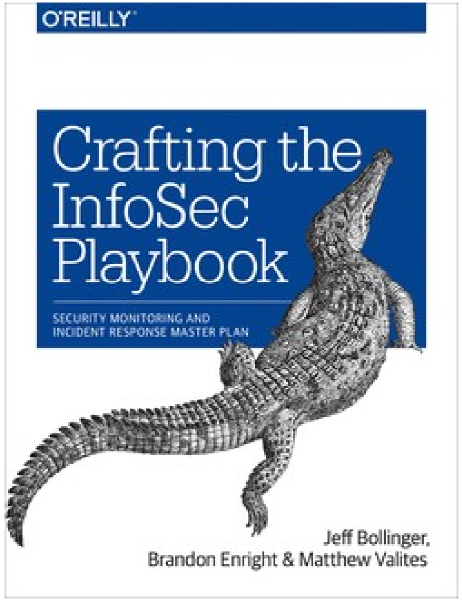
- Improve defensibility
- Focus defenses on threats

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



O'REILLY

Crafting the InfoSec Playbook

SECURITY MONITORING AND
INCIDENT RESPONSE MASTER PLAN

Jeff Bollinger,
Brandon Enright & Matthew Valites

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

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

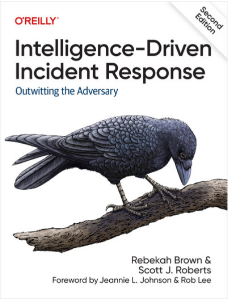
Don’t forget the templates!

Book has some nice templates:

- Short-Form Products
- IOC Report
- Event Summary Report
- Target Package
- Requests for Intelligence
- Long-Form Products

They are in Markdowwn format, so easily used.

Part 3: Summary and finishing up the IDIR book


O'REILLY
Second Edition
Intelligence-Driven Incident Response
Outwitting the Adversary
Rebekah Brown & Scott J. Roberts
Foreword by Jeannie L. Johnson & Rob Lee

Intelligence-Driven Incident Response
Scott Roberts. Rebekah Brown, ISBN: 9781098120689 **2nd edition**- short IDIR

- How did you like the book
- Is it practical
- Let's discuss a bit about learning, and preparing for something unknown

Incident Response

> In the fields of computer security and information technology, **computer security incident management** involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. Computer security incident management is a specialized form of incident management, the primary purpose of which is the development of a well understood and predictable response to damaging events and computer intrusions.[1]

Source: https://en.wikipedia.org/wiki/Computer_security_incident_management
via ”ISO 17799|ISO/IEC 17799:2005(E)”. Information technology - Security techniques - Code of practice for information security management. ISO copyright office. 2005-06-15. pp. 90–94.

- ISO 17799 is superseeded by ISO 27001 and ISO 27002

Exercises

Virtual Machines allowed us play with tech

The following are recommended systems:

- One VM based on Debian, running various software tools
- Setup instructions and help https://github.com/kramse/kramse-labs

Linux is a toolbox we will use and participants will use virtual machines, we also used Windows a few times. Did you notice that a lot of tools for *processing* windows data are running on Linux.

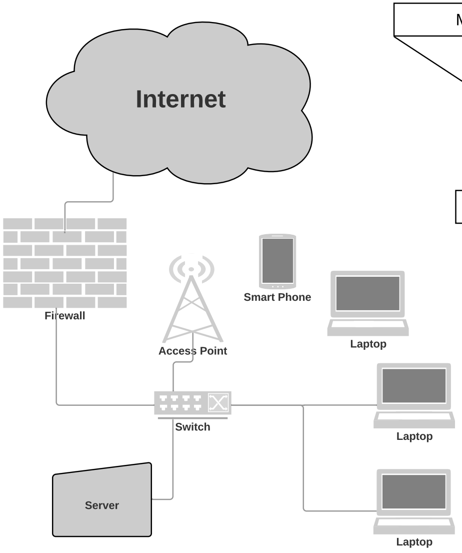
Goals and plans

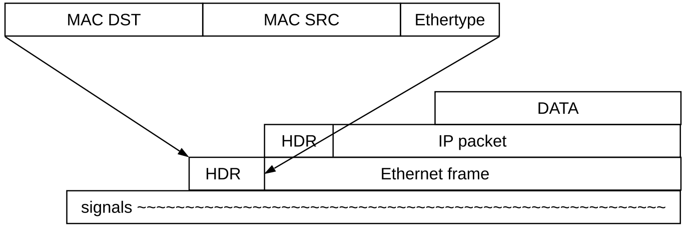
> “A goal without a plan is just a wish.”
> Antoine de Saint-Exupéry

I want this course to

- Include everything listed in contents above
- Be practical – you can do something useful
- Kickstart your journey into Incident Response
  Getting a practical book with pointers about the subject
- Present a lot of useful sources and tools
- Prepare you for production use of the knowledge

Sources: Network overview




MAC DST
MAC SRC
Ethertype
DATA
HDR
IP packet
HDR
Ethernet frame
signals ~~~~~~

Ethernet frames contain packets

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet IPv4 Packet Header

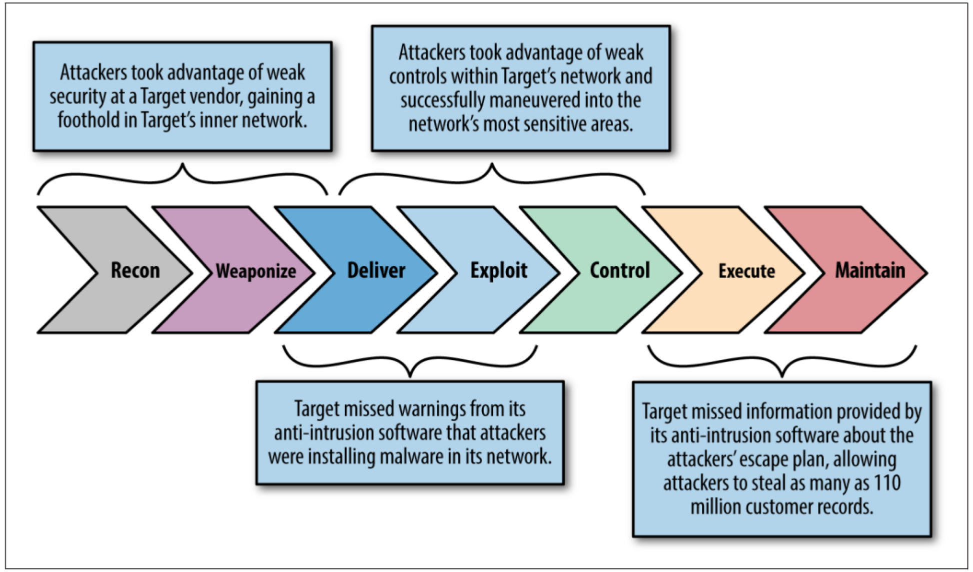
- Internet, routers, firewalls, switches, clients and servers (Wi-Fi not shown)
- Without data we cannot perform Incident Response

Sources: Strategy for implementing identification and detection

We recommend that the following strategy is used for implementing identification and detection – logging:

□ Enable system logging from servers
□ Enable system logging from network devices
□ Enable logging from client devices
□ Centralize logging
□ Add search facilities and dashboards
□ Perform system audits manually or automatically
□ Setup alerting and notification with procedures

Intrusion Kill Chains



Attackers took advantage of weak security at a Target vendor, gaining a foothold in Target's inner network.

Attackers took advantage of weak controls within Target's network and successfully maneuvered into the network's most sensitive areas.

Target missed warnings from its anti-intrusion software that attackers were installing malware in its network.

Target missed information provided by its anti-intrusion software about the attackers' escape plan, allowing attackers to steal as many as 110 million customer records.

Figure 7-1. The kill chain

- See also *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corporation

  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

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**.

Data Analysis Skills

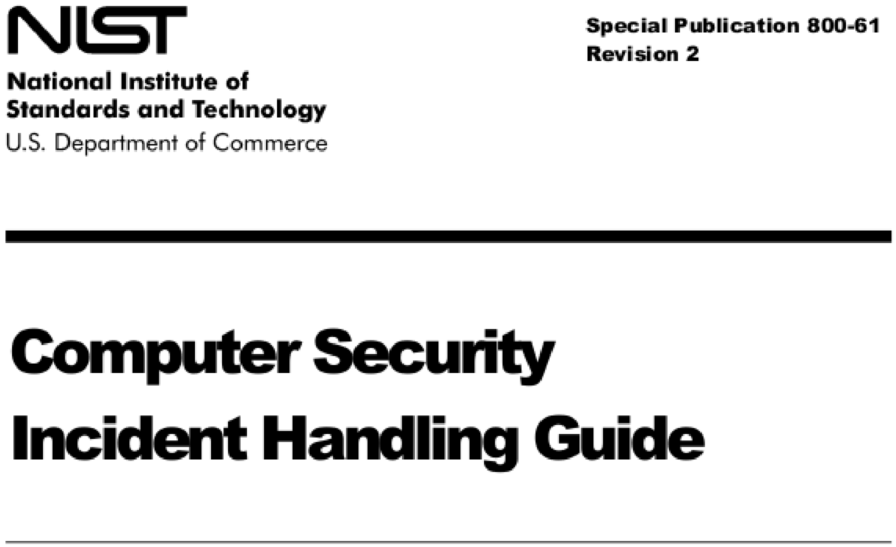
Although we could spend an entire book creating an exhaustive list of skills needed to be a good security data scientist, this chapter covers the following skills/domains that a data scientist will benefit from knowing within information security:

- 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

Part 4: Book: NIST SP800-61rev2



NIST

National Institute of Standards and Technology

U.S. Department of Commerce

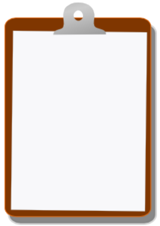
Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

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

Let's dig a bit deeper into this resource

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