Welcome to

Network Monitoring and SIEM

PROSA September 2025

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

Slides are available as PDF, kramse@Codeberg

prosa-network-monitoring-SIEM-2025.tex in the repo security-courses

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teacher and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: hlk@zencurity.com Mobile: +45 2026 6000
- Run a small network for fun AS57860

You are welcome to drop me an email

Code of Conduct

I subscribe to having a Code of Conduct for events, we need them still! Usually I say the BornHack code of conduct apply whenever I teach! https://bornhack.dk/conduct/

Today we talk about networking, so I recommend this also: RIPE Code of Conduct Publication date: 05 Oct 2021

Rationale Our goals in having this Code of Conduct are:

- **To help everyone feel safe and included.** Many people will be new to our community. Some may have had negative experiences in other communities. We want to set a clear expectation that harassment and related behaviours are not tolerated here. If people do have an unpleasant experience, they will know that this is neither the norm nor acceptable to us as a community.
- **To make everyone aware of expected behaviour.** We are a diverse community; a CoC sets clear expectations in terms of how people should behave.

Source: https://www.ripe.net/publications/docs/ripe-766

Time schedule

- 17:00 - 18:15 Introduction and basics for the subject, small exercises
- 18:15 - 18:45 30min break Eat with your family if you like, I will be around most of the break, available for questions
- 18:45 - 19:30 Further teaching and exercises in the subject for the evening
- 15min break Stretch your legs, get some more water
- 19:45 - 20:30 Further teaching and larger exercises in reputation list, SIEM architectures, tools and points
- 20:30 - 21:00 Working with SIEM / SELKS example

I will try to keep this plan for all evenings! So you hopefully can plan family life better

Will also try to make smaller breaks/exercises during the slidesshows, check for questions etc.

Modul 3: Netværksovervågning og SIEM (Onlinemodul 3 af 3)

Hvordan kan vi overvåge netværk effektivt?

SIEM er et bredt udtryk for systemer, der kan samle information om sikkerhedsevents og netværksdelen er særligt interessant. I dette modul får du præsenteret grundsten som Netflow samt værktøjer til at generere, opsamle og præsentere disse data effektivt med grafiske værktøjer, som kan tilgås via browser. Og måske i visse tilfælde kunne automatiseres med Machine Learning, som ikke er en del af oplægget.

Keywords: CIA modellen, CVE sårbarheder, switch, router, firewall, ACL, DoS/DDoS, VLAN, segmentering, **logning, monitoring, Netflow, Zeek, Suricata, Elasticsearch**, Nmap, IEEE 802.1x, IPv4, IPv6, NTP, DNS

- Vi skal prøve at få et overblik over hvad vi har lært hidtil
- Hvordan kan vi bruge den viden vi samler op effektivt
- Alle værktøjer der præsenteres er veldokumenterede mange steder – inkl videoer

Goals for today

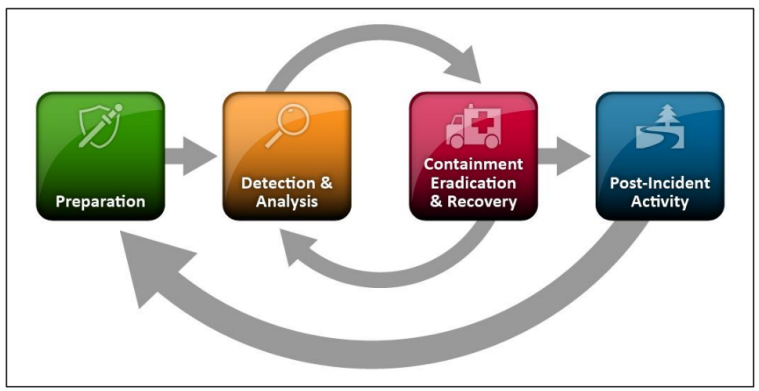
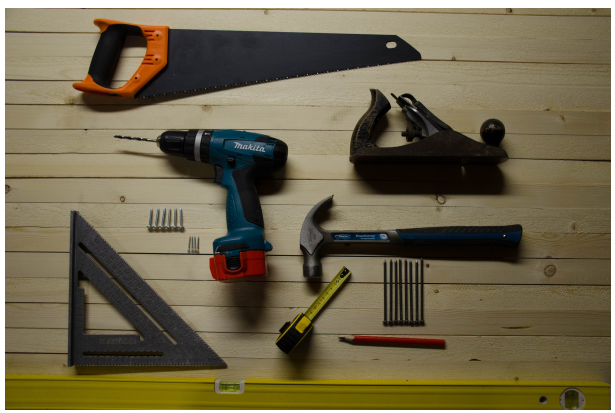


Figure 3-1. Incident Response Life Cycle

- Make sure we have an overview of SIEM terms, including NSM
- Have a big picture of how a network can be more secure after applying the methods in these modules
- Put the icing on the cake – see beautiful pictures

Exercises are completely optional



- See references to various tools and utilities
- See MISP and try if you like
- See SELKS and try if you like

Linux is a toolbox I will use and participants are free to use whatever they feel like Photo by Eugen Str on Unsplash

What is a Secure Network

A controlled environment with a purpose and goal which is designed, implemented and monitored to be sufficiently secure – according to the policies and wishes of the owner and operator

Example networks

- Home network – should support a *family typically*
- Factory network – should support machines, robots, production of things
- Office network – should be available for employees and without malware and data leaks

Network Security as a Holistic Approach

holistic adjective

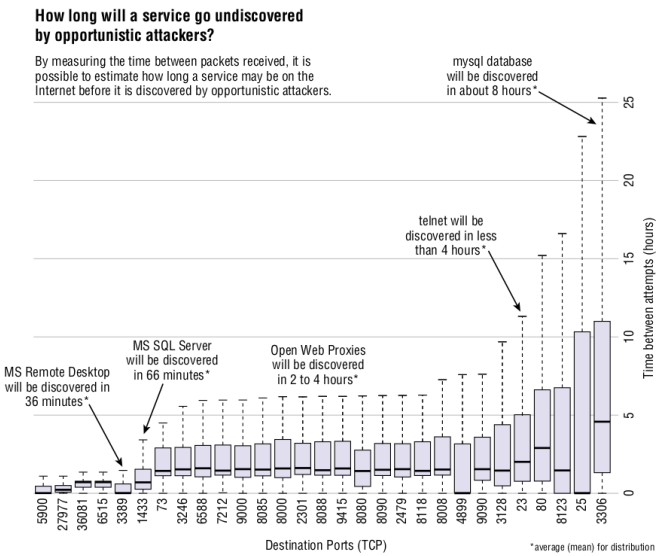
1 : of or relating to holism

2 : relating to or concerned with wholes or with complete systems rather than with the analysis of, treatment of, or dissection into parts
holistic medicine attempts to treat both the mind and the body
holistic ecology views humans and the environment as a single system

Source: https://www.merriam-webster.com/dictionary/holistic

- The network spans the whole organisation and we use *the network* – the Internet for many things
- Network security affects the whole organisation
- When improving network security, we often improve overall security

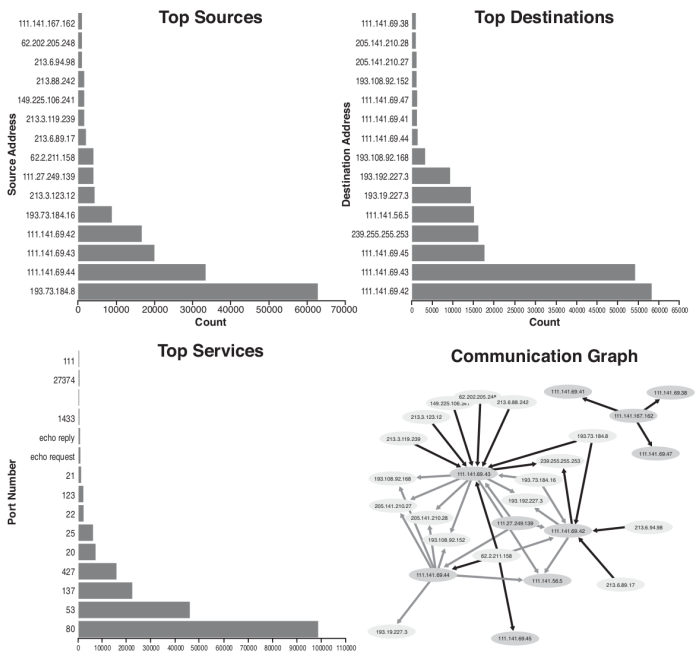
Example plot 6-17



Source: DDS 6. Visualizing Security Data

- Interesting graph, and interesting results Changing away from standard ports delay attackers!
- Attackers are constantly scanning – internet tinnitus

Applied Security Visualization examples



Source: Network Flow Data in *Applied security visualization*, Rafael Marty, 2009

CIP 1 Incident Response Fundamentals

- Keeping an organization safe from attack, as well as having a **talented team** available to **respond quickly, minimizes damage** to your reputation and business.
- Fostering and developing **relationships** with IT, HR, legal, executives, and others is critical to the success of a CSIRT.
- **Sharing incident and threat data** with external groups improves everyone's security and gives your organization credibility and trust with groups that might be able to help in the future.
- A good team relies on good tools, and a great team optimizes their operations.
- A solid and well-socialized InfoSec policy gives the incident response team the authority and charter to protect networks and data.

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

CIP 2 What Are You Trying to Protect?

- **You can't properly protect your network if you don't know what to protect.**
- Define and understand your **critical assets** and what's most important to your organization.
- Ensure that you can attribute **ownership or responsibility for all systems on your network.**
- Understand and leverage the log data that can help you determine host ownership.
- A complex network is difficult to protect, unless you understand it well.

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

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

- I recommend *Modern Security Operations Center, The* ISBN: 978-0135619858 Joseph Muniz - short SOC
  If you need to build a SOC, that is great source of information

Data Driven vs Intelligence Driven

What is the difference? Data Driven, Intelligence Driven, Network Security Monitoring

Short description

- Network Security Monitoring is what we do, with tools like Zeek, Suricata, logging tools
- Data Driven is when we use that data: start blocking, investigate incidents based on alerting
- It becomes intelligence when we share it with other: sharing a list of systems that tried brute-forcing our services
- They become Intelligence Driven when they use processed sources: block lists, IoC etc.
- We become Intelligence Driven when we use data sources from others

TL;DR Don't worry, use tools, resources and anything that you can!

Network security monitoring (NSM)

> Network security monitoring (NSM) is the collection and analysis of network data such as logs, traffic patterns, and anomalies. Security professionals use this data to discover and respond to potential intrusions and malicious activity.

Source: https://corelight.com/resources/glossary/network-security-monitoring-nsm

- Note: they are selling commercial product Open NDR based on Zeek, Suricata and Sigma SIEM rules

Data-Driven

data-driven / de tə dr vn, d tə dr vn/ adjective
determined by or dependent on the collection or analysis of data. "decisions are data-driven and made by committee"

Source: Oxford Languages

- Was the preferred term a few years back
- Today everything is *intelligence* – see also Artificial Intelligence (AI)
- You need data to be able to make evidence-based decisions and perform actions

Intelligence in network security

> **Intelligence is derived from a process of collecting, processing, and analyzing data.** Once it has been analyzed, it **must be disseminated** in order to be useful. Intelligence that does not get to the right audience is wasted intelligence. Wilhelm Agrell, a Swedish writer and historian who studied peace and conflict, once famously said, "Intelligence analysis combines the dynamics of journalism with the problem solving of science."

Source: IDIR 2. Basics of Intelligence
Intelligence-Driven Incident Response (IDIR)
Scott Roberts. Rebekah Brown

- Sharing data helps us and others
- We can use many sources of data to enable quicker response

Intelligence-driven computer network defense

> Intelligence-driven computer network defense is a risk management strategy that addresses the threat component of risk, incorporating analysis of adversaries, their capabilities, objectives, doctrine and limitations. This is necessarily a continuous process, leveraging indicators to discover new activity with yet more indicators to leverage. It requires a new understanding of the intrusions themselves, not as singular events, but rather as phased progressions. This paper presents a new intrusion kill chain model to analyze intrusions and drive defensive courses of action.

Source: *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

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Intrusion Kill Chains

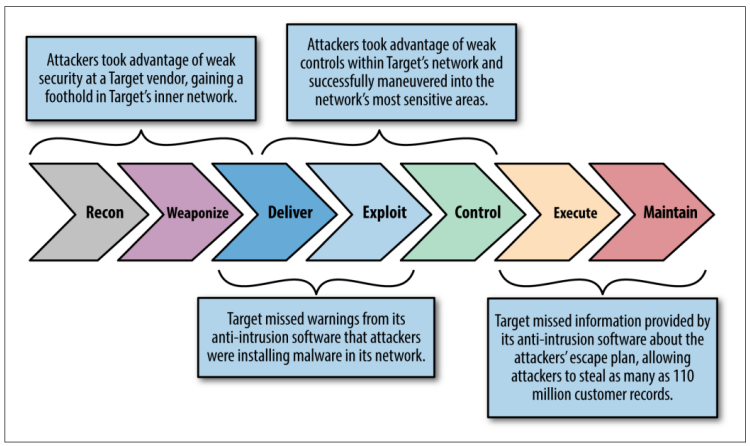


Figure 7-1. The kill chain

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

Indicators of Compromise and Signatures

An IOC is any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner. This could include a simple indicator such as the IP address of a command and control (C2) server or a complex set of behaviors that indicate that a mail server is being used as a malicious SMTP relay.

When an IOC is taken and used in a platform-specific language or format, such as a Snort Rule or a Zeek-formatted file, it becomes part of a signature. A signature can contain one or more IOCs.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

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

Data-Driven Security: Analysis, Visualization ...

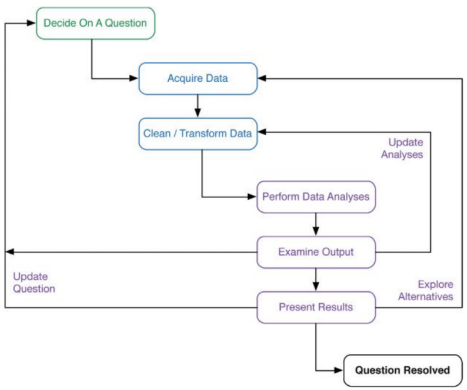


FIGURE 12-2 *The data science workflow*

- Find and Collect Relevant Data
- Learn through Iteration
- Find Statistics

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

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 overview JSON

> JavaScript Object Notation (JSON, pronounced / d e sən/; also / d e s n/[note 1]) is an open-standard file format or data interchange format that uses **human-readable text** to transmit data objects consisting of attribute–value pairs and array data types (or any other serializable value). It is a very common data format, with a diverse range of applications, such as serving as replacement for XML in AJAX systems.[6]

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

- I like JSON much better than XML
- Many web services can supply data in JSON format

The Zeek Network Security Monitor

Together with firewalls – The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework

The Zeek Network Security Monitor

> While focusing on network security monitoring, Zeek provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Zeek has successfully bridged the traditional gap between academia and operations since its inception.

Zeek is the tool formerly known as Bro, changed name in 2018. https://www.zeek.org/

Suricata IDS/IPS/NSM

Together with firewalls – Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

https://suricata.io https://openinfosecfoundation.org

Zeek, Suricata, JSON and jq


```
{
  "timestamp": "2008-07-22T03:51:08.386060+0200",
  "flow_id": 1376641579994488,
  "pcap_cnt": 67,
  "event_type": "dns",  "proto": "UDP",
  "src_ip": "192.168.1.64",  "src_port": 27440,
  "dest_ip": "192.168.1.254",  "dest_port": 53,
  "pkt_src": "wire/pcap",
  "dns": {
    "version": 2,
    "type": "query",
    "id": 11992,
    "rrname": "ssl-google-analytics.l.google.com",
    "rrtype": "AAAA",
    "tx_id": 0,
    "opcode": 0
  }
}
```


- `hlk@debian-lab:~/suri$ cat eve.json | jq | head -21` jq is a lightweight and flexible command-line JSON processor https://jqlang.org/

Commercial Support

You can and should use updated rulesets for Suricata.

I Recommend the Emerging Threats ET Pro ruleset

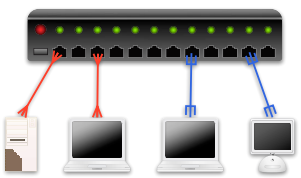
Metadata – enrichment

Metadata	Metacategory: Data
The DNS lookup occurred at a certain time.	Timestamp: 278621182
The internal host sent a DNS PTR request.	Network protocol: DNS PTR
The internal host had a hostname.	Location: Desktop subnet
	Source IP Address: 1.1.1.2
	Hostname: windowspc22.company.com
The internal host resolved an external host.	Location: External
	Destination IP Address: 255.123.215.3
	Hostname: dgf7adfnkjhh.com
The external host was hosted by a dynamic DNS provider.	Network: Shady DDnS Provider Inc.
	ASN: SHADY232
	Reputation: Historically risky network
The remote hostname appeared randomly generated.	Hostname: dgf7adfnkjhh.com
	Category: Unusual, nonlinguistic

Source: picture from Crafting the InfoSec Playbook, CIP

Metadata + Context

Reputation-Based Detection



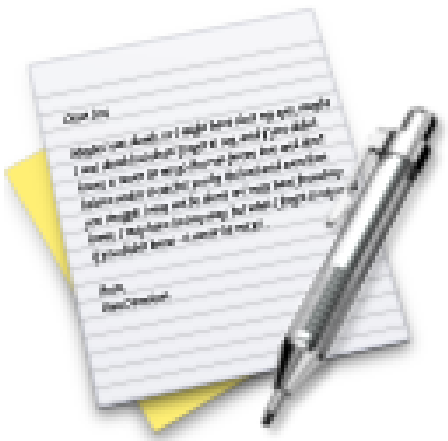
- The most basic form of intrusion detection is reputation-based detection
- Similar concept to block lists for SMTP spam relays
- I often recommend https://github.com/stamparm/maltrail as a source of lists
- Other sources are lists like RIPE NCC delegated, which IP prefixes are handed out in different countries
  https://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-extended-latest
  `ripencc|DK|ipv4|185.129.60.0|1024|20151130|allocated|`
- Should we trust all danish network companies?
  Probably not, but we can easily get into contact with them and report *bad servers*

IP reputation

Zeek documentation Intel framework
https://docs.zeek.org/en/stable/frameworks/intel.html

Suricata reputation support
https://suricata.readthedocs.io/en/latest/reputation/index.html

Exercise



Now lets do the exercise

⚠ IP address research 15 min

which is number **31** in the exercise PDF.

Exercise

Now lets do the exercise

⚠ Data types: IP reputation – 15min

which is number 32 in the exercise PDF.

November 2021: Log4Shell CVE-2021-44228

It would not be possible to discuss 2021 in the context of vulnerabilities without the mention of Log4Shell. **A widely used Java-based logging library caused headaches for Security professionals worldwide**. Many scrambled to quantify their use of Log4j within their estates.

A zero-day exploit quickly followed, confirming the worst - **Remote Code Execution (RCE) was indeed possible.** However, what made the nature of the vulnerability even more challenging was the ability to exploit a backend logging system from an unaffected front end host. For example, an attacker can craft a weaponised log entry on a mobile app or webserver not running Log4j. The attacker could make their way through to backend middleware itself running Log4j, which significantly extends the attack surface of the vulnerability.

The NCSC even took the step of recommending the update was immediately applied, whether or not Log4Shell was known to be in use. As is commonly the case with critical vulnerabilities, two successive Log4j patches were subsequently released in the week following the original addressing Denial of Service (DoS) and a further RCE. This further increased workloads of Security and IT teams just as they thought the worst of 2021 had been and gone.

Source - for this description:
https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/

See also https://en.wikipedia.org/wiki/Log4Shell

CrowdSec – Crowd sourced security information

Detect and block Log4j exploitation attempts with CrowdSec

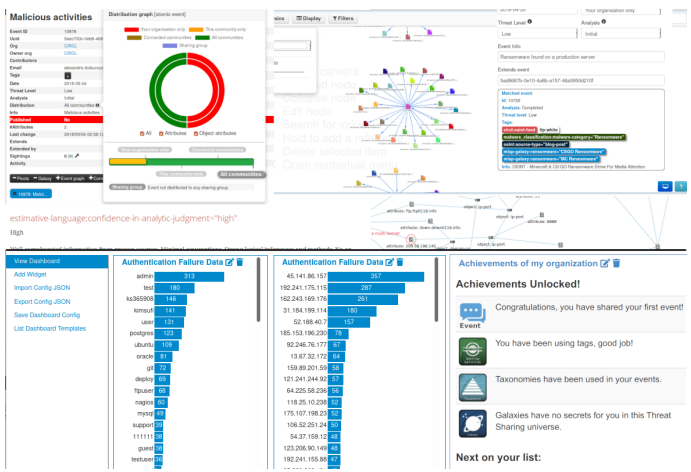
If you work in Infosec, you had a very lousy weekend. And that's because of the Log4j zero-day vulnerability (CVE-2021-44228) that was discovered. We had no choice but to roll up our sleeves to help our community before things got messier than they already were.

As a result, we have released a scenario that will help you detect and block exploitation attempts of the vulnerability. This new scenario can be directly downloaded from our Hub and installed in a blink of an eye. Check this quick video to see the plugin in action:

https://www.crowdsec.net/blog/detect-block-log4j-exploitation-attempts

- Log4j is a popular software library in the Java world
- CrowdSec quickly provided a list of systems scanning the internet for this vulnerability
- Full disclosure they gave me a hoodie at an event ☺

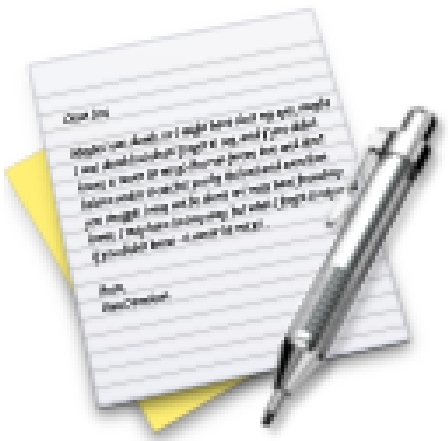
Research MISP Project 30min



Demo and Research the MISP Project. Running MISP Project is will allow you to fetch reputation lists easily and analyse logs better

Suggested method if you want to try it: https://www.misp-project.org/download/
I use the *Production ready docker images for MISP and MISP-modules*

Exercise

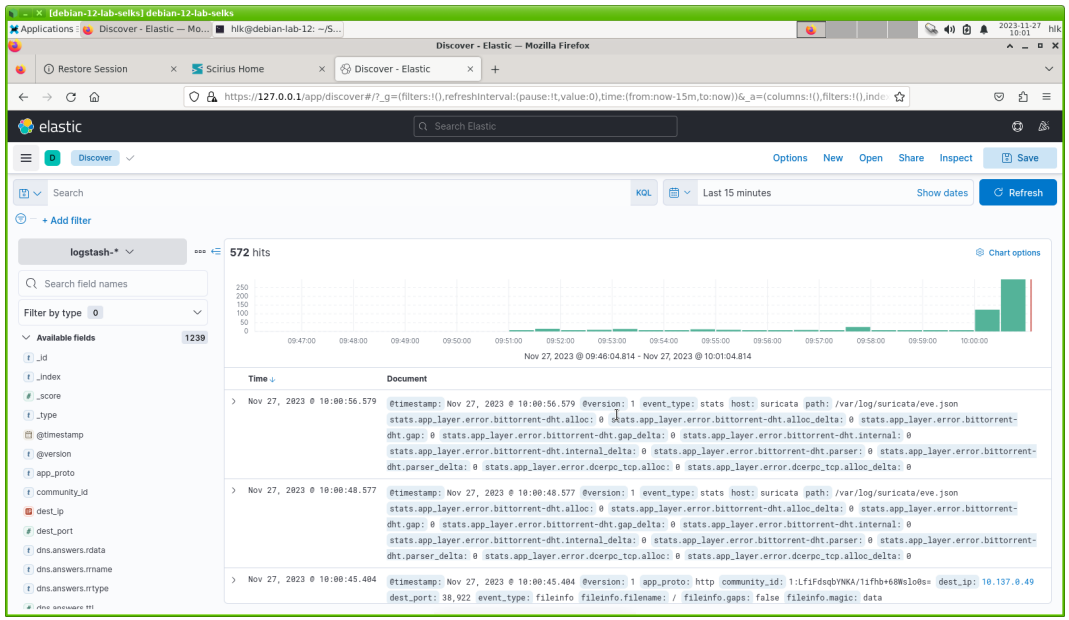


Now lets do the exercise

Research MISP Project 30min

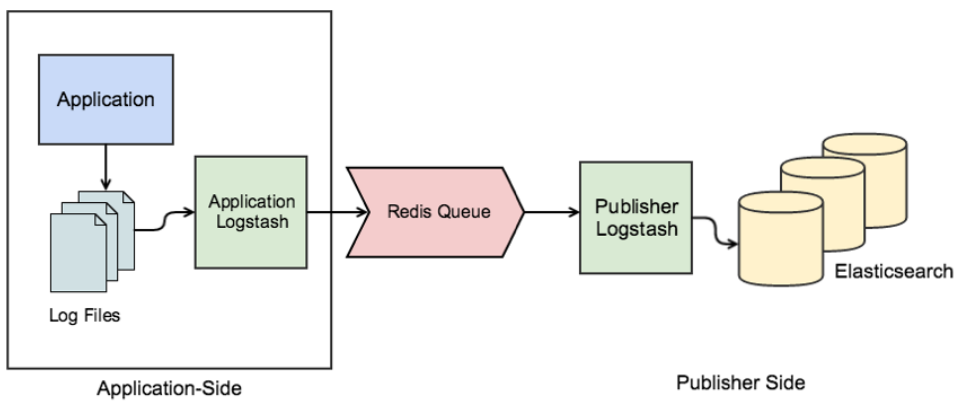
which is number 33 in the exercise PDF.

Dashboards and Searching



- Some of the most important parts of a SIEM is searching and dashboards

SIEM Architecture and Storage platform ElasticSearch!



Note: Kibana makes it easy to use sample data, feel free to experiment!

Elasticsearch and Kibana are *services* which open a listening socket/port. So access ES via https://127.0.0.1:9200 and Kibana via https://127.0.0.1:5601 on your Debian using a browser or Postman

Using the SELKS Docker images are the easiest way

Example data store: Elasticsearch

> Elasticsearch is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java.

Source: Wikipedia https://en.wikipedia.org/wiki/Elasticsearch

- Initial release 8 February 2010
- Open core means parts of the software are licensed under various open-source licenses (mostly the Apache License)
- Various browser tools and plugins for ES exist, to make life easier
- I often use ES for storing Log Messages and Events from multiple systems, a SIEM Security information and event management.

Elasticsearch

> **ElasticSearch consumes practically anything you give it** and provides straightforward ways to ask it questions and get data out of it. You just need to feed it **semi- or unstructured data** and fold in some domain intelligence to enable smart indexing. It works its multi-node NoSQL magic in conjunction with **a layer of full-text searching** to give you **almost instantaneous query results even for large amounts of data.**
> Source: DDS 8. Breaking Up with Your Relational Database

- Elasticsearch SIEM – from Elastic
- Wazuh – agent for clients, log events, integrity protection etc.
- HELK – all-in one hunting system
- ElastiFlow – netflow system
- Arkime (renamed recently from Moloch) – packet capture

Lots of commercial systems, and lots of companies providing cloud logging platform

Microsoft Azure promotes Sentinel – cloud based SIEM

https://azure.microsoft.com/da-dk/services/azure-sentinel/

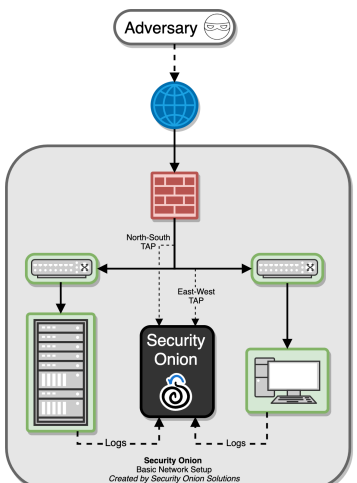
Elasticsearch SIEM

Elastic Common Schema (ECS)

The Elastic Common Schema (ECS) defines a common set of fields for ingesting data into Elasticsearch. A common schema helps you correlate data from sources like logs and metrics or IT operations analytics and security analytics.

- Some structure is useful, Elastic Common Schema (ECS)
  https://github.com/elastic/ecs
- I would use their schemas for a green field deployment,
  as they have been expanded and developed over some time
- Correlation becomes implicit in every search!
  – hint/fact from https://www.elastic.co/webinars/introducing-the-elastic-common-schema

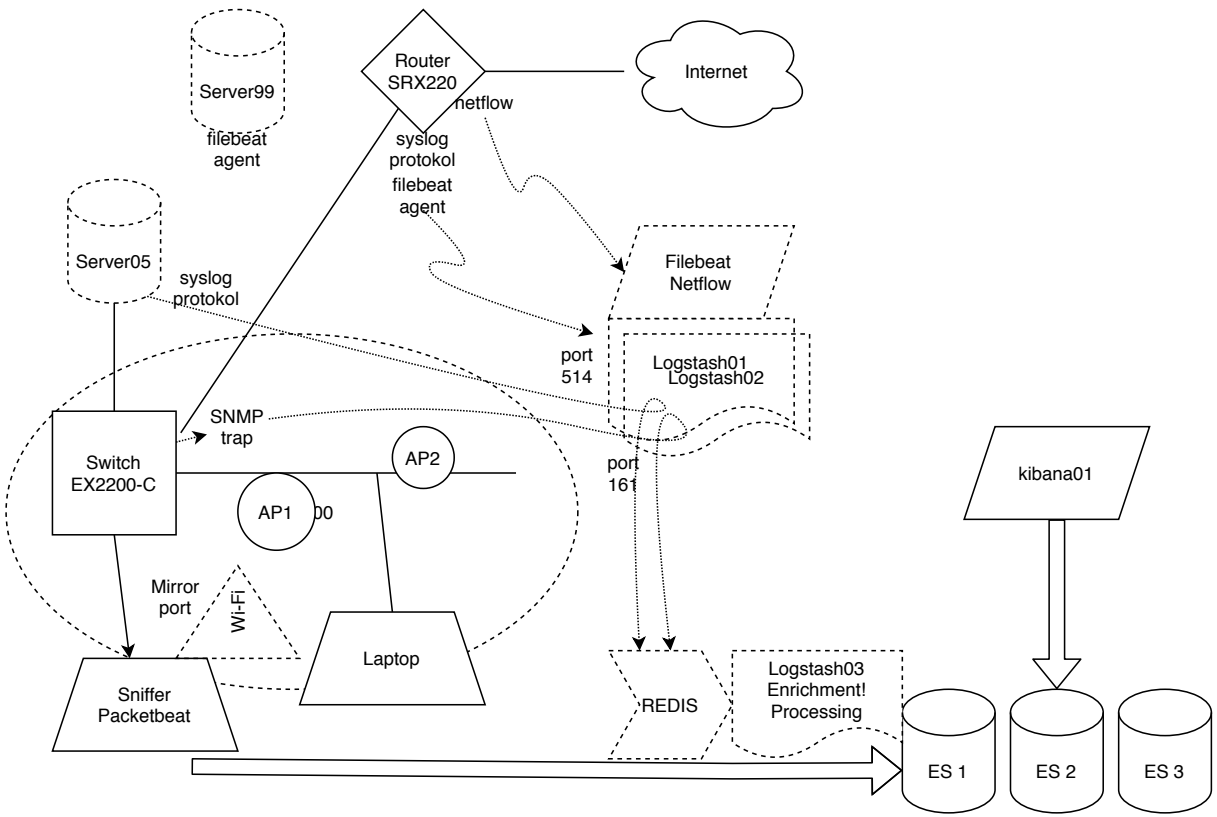
Architecture for packet capture



Security Onion is a free and open platform built by defenders for defenders. It includes network visibility, host visibility, intrusion detection honeypots, log management, and case management.

Source: https://docs.securityonion.net/en/2.4/introduction.html

Lets design a SIEM Infrastructure Proof of Concept



Summary Processing of Data in the SIEM world

Let's look at some processing

- Processing includes normalizing collected data into uniform formats for analysis
- Indexing – Large volumes of data need to be made searchable
- Translation – for our course we might get multiple input formats but need JSON or XML
- Enrichment – Providing additional metadata for a piece of information is important. For example, domain addresses need to be resolved to IP addresses, and **WHOIS registration data fetched**
- Filtering – Not all data provides equal value, and analysts can be overwhelmed when presented with endless streams of irrelevant data
- Prioritization – The data that has been collected may need to be ranked so that analysts can allo- cate resources to the most important items
  Note: this relates to a *baseline*, what errors are normal in your environment
- Visualization – Data visualization has advanced significantly and the human eye and brain can often see patterns

SELKS – now Clear NDR

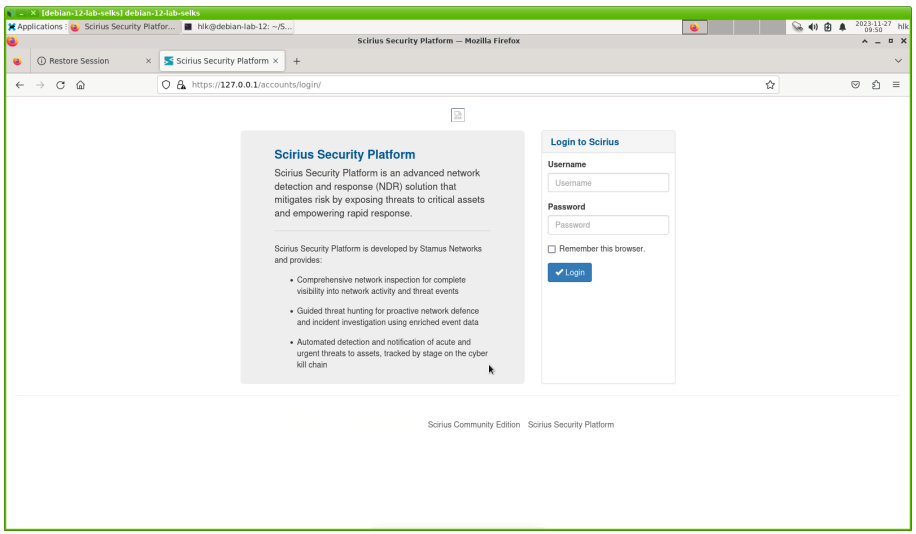
> SELKS™ is a free, open-source, and turn-key Suricata network intrusion detection/protection system (IDS/IPS), network security monitoring (NSM) and threat hunting implementation created and maintained by Stamus Networks.

Source: https://www.stamus-networks.com/blog/selks-10-the-next-big-leap-for-open-source-network-security

- Suricata - Ready to use Suricata
- Elasticsearch - Search engine
- Logstash - Log injection
- Kibana - Custom dashboards and event exploration
- Stamus C.E. (formerly Scirius) - Suricata ruleset management and Suricata threat hunting interface

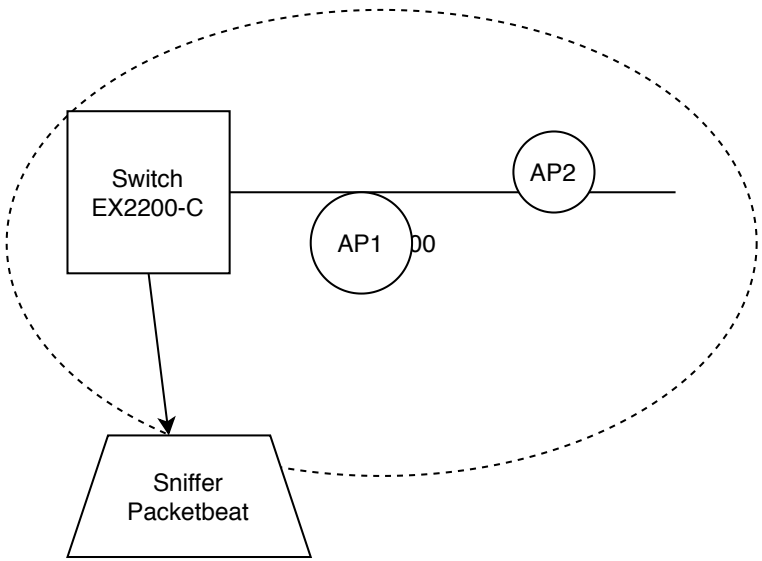
https://github.com/StamusNetworks/SELKS

SELKS 10 (now Clear NDR - Community)



- Description for this setup is in the Kickstart 2 document
- Using Docker we can turn up a full installation of Elasticsearch with data in minuts!
- https://github.com/StamusNetworks/SELKS

Packetbeat as an alternative

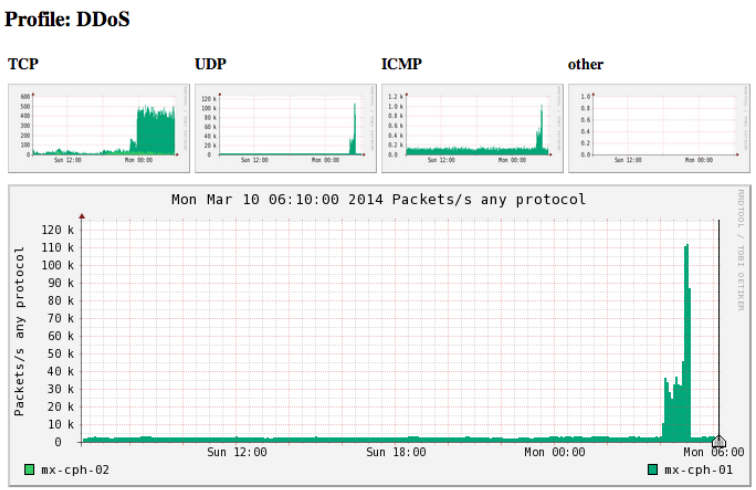


- By installing packetbeat and doing network mirroring from the network switch, we can gather a lot of information
- Packetbeat supports Elastic Common Schema (ECS) https://www.elastic.co/beats/packetbeat
- ICMP (v4 and v6) DHCP (v4) DNS HTTP AMQP 0.9.1 Cassandra Mysql PostgreSQL Redis Thrift-RPC MongoDB Memcache NFS TLS SIP/SDP (beta)

Running SELKS

I will run this first, then we will discuss the tools and related questions

Baseline

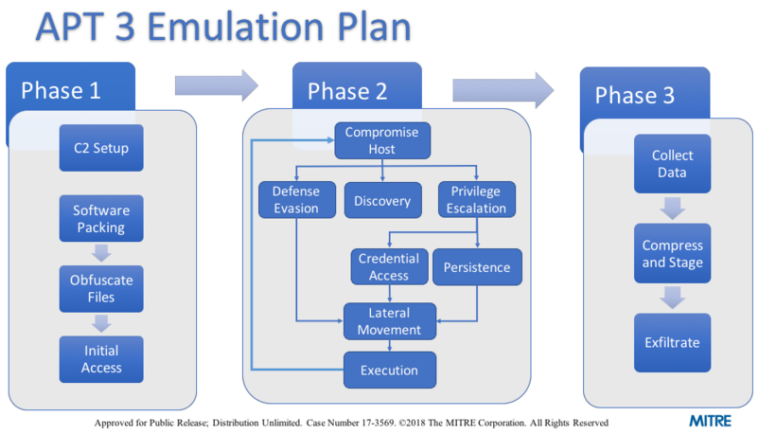


- Picture from NFsen running a specific profile to catch attacks
- When you have a running system, it will start to gather a baseline
- Comparing data from various times become possible, and usefull
- The best baseline is from running the actual systems and services for an extended *learning* period

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

MITRE Adversary Emulation Plans



To showcase the practical use of ATT&CK for offensive operators and defenders, MITRE created Adversary Emulation Plans. These are prototype documents of what can be done with publicly available threat reports and ATT&CK.

Source: https://attack.mitre.org/resources/adversary-emulation-plans/

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

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

Buy or DIY?

> DNSDB is a database that stores and indexes both the passive DNS data available via Farsight Security's Security Information Exchange as well as the authoritative DNS data that various zone operators make available.

Source: from https://docs.dnsdb.info/

- Excellent services can be bought, have used https://team-cymru.com/
- Compare using https://docs.dnsdb.info/ Farsight DNSDB API documentation
- Lots of examples for adding functionality, building and expanding SIEM and log systems
- I usually go to Github and have found a lot of useful tools

Team Cymru

We operate as our own ISP and are part of the fabric of the internet. We've amassed an unmatched number of data sharing partnerships with operators worldwide, in addition to gathering threat intelligence from a global grid of sensors, honeypots, darknets and crawlers. We give you our visibility via our Pure Signal™ platform, Augury™.

- Trace threat actors through dozens of proxies and VPNs.
- Map the extended infrastructure.
- Preemptively block associated IPs.
- Then monitor these threats to defend against them indefinitely.

Source: from https://team-cymru.com/

- Often you need sources that are hard to get
- Many vendors integrate sources into other products too
- Firewalls and Load balancing products that include reputation lists

The Spamhaus Don't Route Or Peer Lists

> The Spamhaus Don't Route Or Peer Lists
> DROP (Don't Route Or Peer) and EDROP are advisory "drop all traffic"lists, consisting of stolen 'hijacked' netblocks and netblocks controlled entirely by criminals and professional spammers. DROP and EDROP are a tiny subset of the SBL designed for use by firewalls and routing equipment.

http://www.spamhaus.org/drop/

- When your SIEM alerts you, you need tools to block and restrict
- Recommend adding empty blocking access control lists etc. to your network infrastructure
- Add premade blocking to your name servers, proxy servers, recursive servers
- Recommend implementing country lists

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

Source: NIST-SP800-61r2.png

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

Incident Response Life cycle

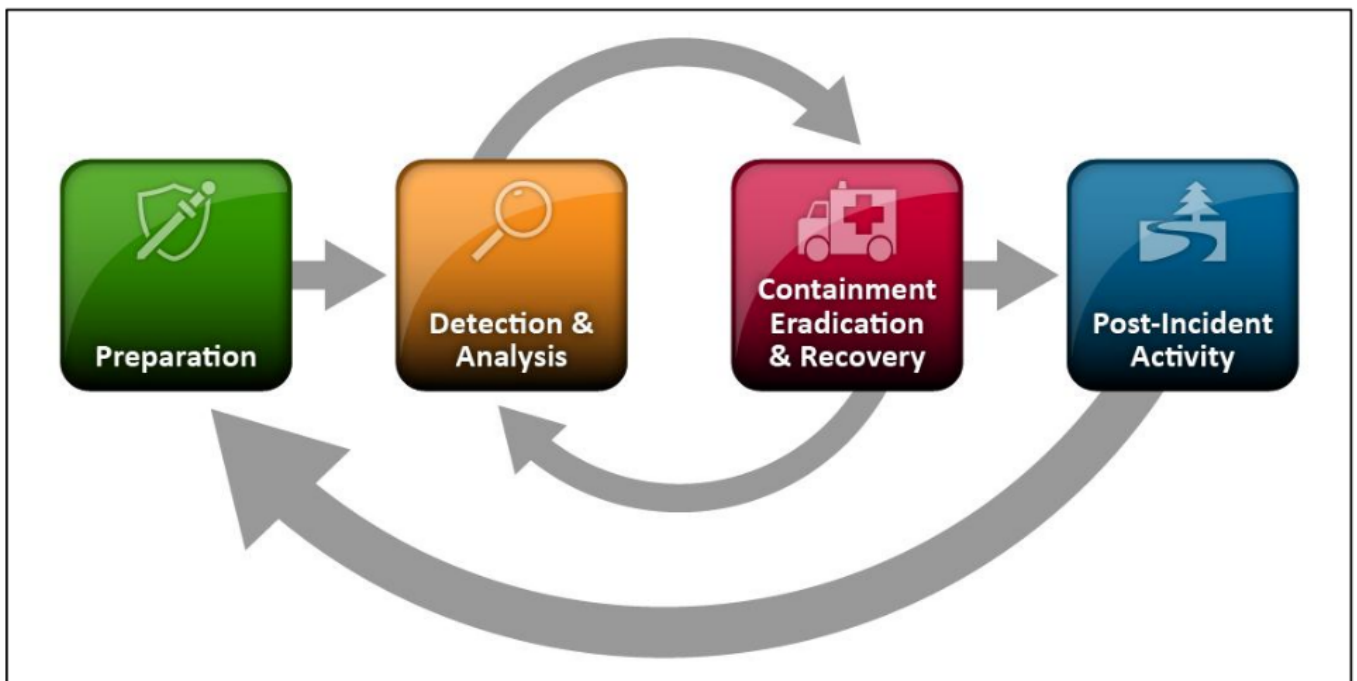


Figure 3-1. Incident Response Life Cycle

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

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

Mitigate

> Mitigation is the process of taking **temporary steps** to keep an intrusion from **getting worse** while **longer-term corrections** are taken. Ideally, mitigation should take place **quickly and in a coordinated fashion** to avoid giving the adversary a chance to react before you have cut off their access. Mitigation takes place at several phases of the **kill chain**, including delivery, command and control, and actions on target.

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

- Stop the delivery by blocking known entry ways
- Patch remaining systems – to avoid new infections
- Block known bad IP addresses

Remediate

> Remediation is the process of **removing all adversary capabilities and invalidating any compromised resources** so that they can no longer be used by the adversary to conduct operations. **Remediation** generally focuses on a different set of kill-chain phases than mitigation does, most notably **exploitation, installation, and actions over target**, which we will break down in this section.

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

- Clean and Patch systems

Rearchitect

> One of the most effective uses of **intelligence-driven incident-response data** is an advanced form of remediation: the incident-response team looks at **past incident trends, identifies common patterns, and works to mitigate these at a strategic level**. These mitigations are generally not small changes, and may range from small things like tweaks to system configurations or additional user training, to massive shifts in tooling such as the development of a new security tools or even complete network rearchitecture.

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

- Why did the attacks succeed in the first place, can we change the environment

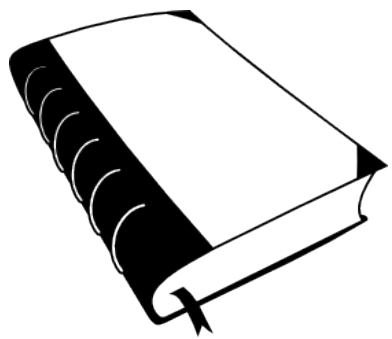
Conclusion

I hope you learnt something about firewalls, network security, protocols – how it helps keep the network secure, and monitoring for intrusions that are bound to happen

- Implement firewalls – take control over network packets, flows, protocols, services etc. also to reduce noise!
- Start monitoring with available data feed, sources, netflow, firewall logging, DNS queries etc.
- Start from the bottom and from client ports, or from server ports if you like
- UNIX and Linux are example systems – and often found in appliances
  Learn some Linux and use open source projects, really, will save you thosands of USD/EUR/DKK
  or you can decide to outsource this, your choice, but make it a well reasoned choice

Primary literature used in the course SIEM and Log Analysis

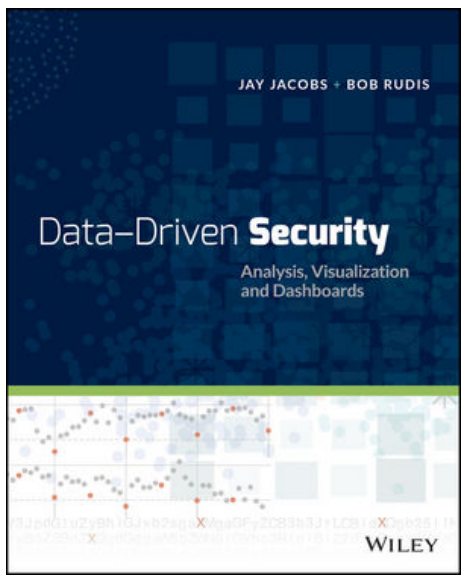
Primary literature:



Free graphics by Lumen Design Studio

- *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. Rebekah Brown, ISBN: 9781098120689 **2nd edition**- short IDIR
- *Modern Security Operations Center, The* ISBN: 978-0135619858 Joseph Muniz - short SOC

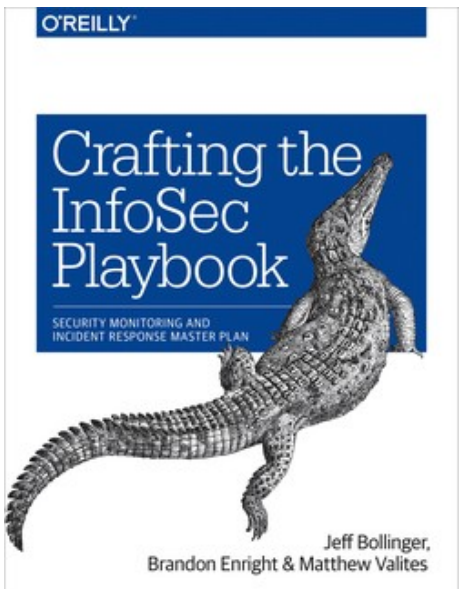
Data-Driven Security: Analysis, Visualization and Dashboards



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

Our main book for this course. We will read a lot from this one. From basic data processing to dashboards

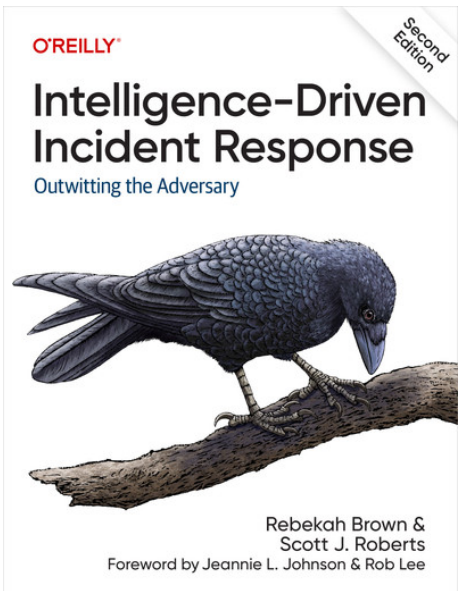
Crafting the InfoSec Playbook



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

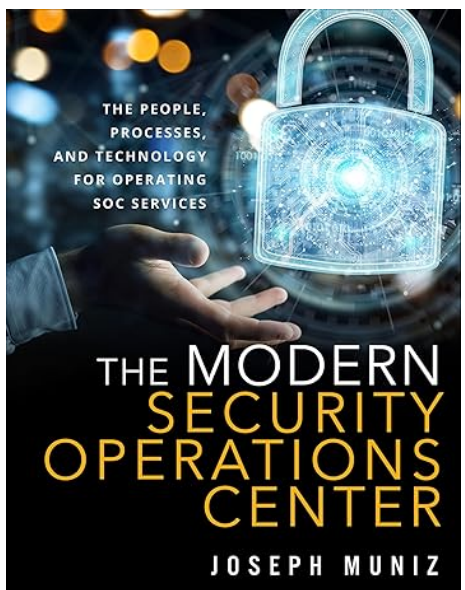
Develop your own threat intelligenceand incident detection strategy

Intelligence-Driven Incident Response



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

Security Operations Center

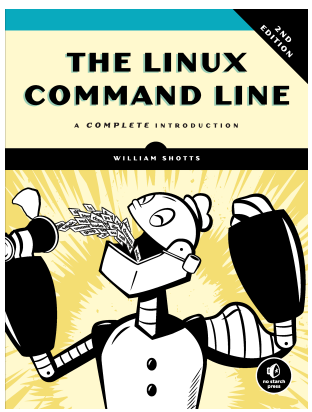


Modern Security Operations Center, The
ISBN: 978-0135619858 Joseph Muniz - short SOC

Supporting literature books

- *The Linux Command Line: A Complete Introduction*, 2nd Edition
  by William Shotts
- *The Debian Administrator's Handbook*, Raphaël Hertzog and Roland Mas
  https://debian-handbook.info/ - shortened DEB

Book: The Linux Command Line



The Linux Command Line: A Complete Introduction , 2nd Edition by William Shotts

Print: https://nostarch.com/tlcl2
Download – internet edition https://sourceforge.net/projects/linuxcommand
Not curriculum but explains how to use Linux

The Debian Administrator's Handbook (DEB)

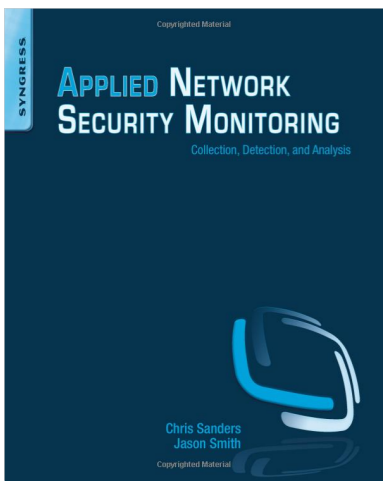
The Debian Administrator's Handbook, Raphaël Hertzog and Roland Mas
https://debian-handbook.info/ - shortened DEB

Primary literature used in the course Communication and Network Security

Primary literature are these three books:

- *Applied Network Security Monitoring Collection, Detection, and Analy sis*, 2014 Chris Sanders ISBN: 9780124172081 - shortened ANSM
- *Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems*, 3rd edition 2017, Chris Sanders ISBN: 9781593278021 - shortened PPA

Book: Applied Network Security Monitoring (ANSM)

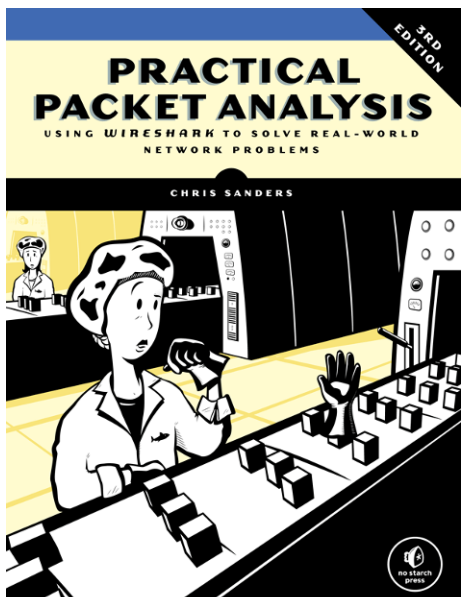


Applied Network Security Monitoring: Collection, Detection, and Analysis 1st Edition

Chris Sanders, Jason Smith eBook ISBN: 9780124172166 Paperback ISBN: 9780124172081 496 pp. Imprint: Syngress, December 2013

https://www.elsevier.com/books/applied-network-security-monitoring/unknown/978-0-12-417208-1

Book: Practical Packet Analysis (PPA)



Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition April 2017, 368 pp. ISBN-13: 978-1-59327-802-1

https://nostarch.com/packetanalysis3