Session 4: Computer Network Defense, The Big Picture 1

COINS Summer school 2018,
Metochi, Greece

Christoffer V. Hallstensen

Overview

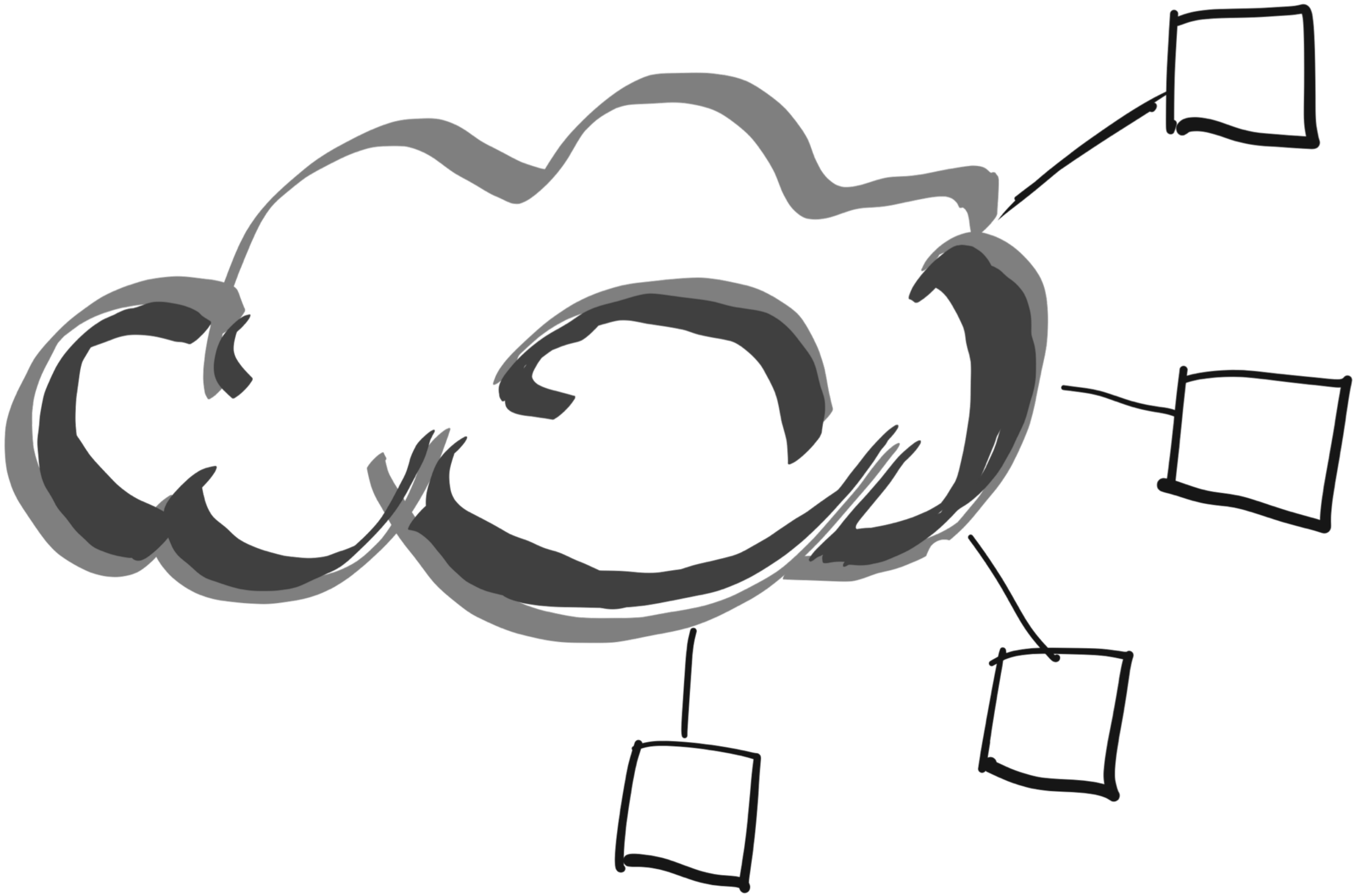
- Session 4 (24.07 17:00 – 19:00)
  - Problemspace: Defense Complexity
  - **Protecting**: Network defense requirements
  - **Detecting**: Network Security Monitoring (NSM)
- Session 5 (25.07 09:00 – 11:00)
  - **Reponding**: Security Analytics and DFIR
  - **Sustaining**: Security Operations

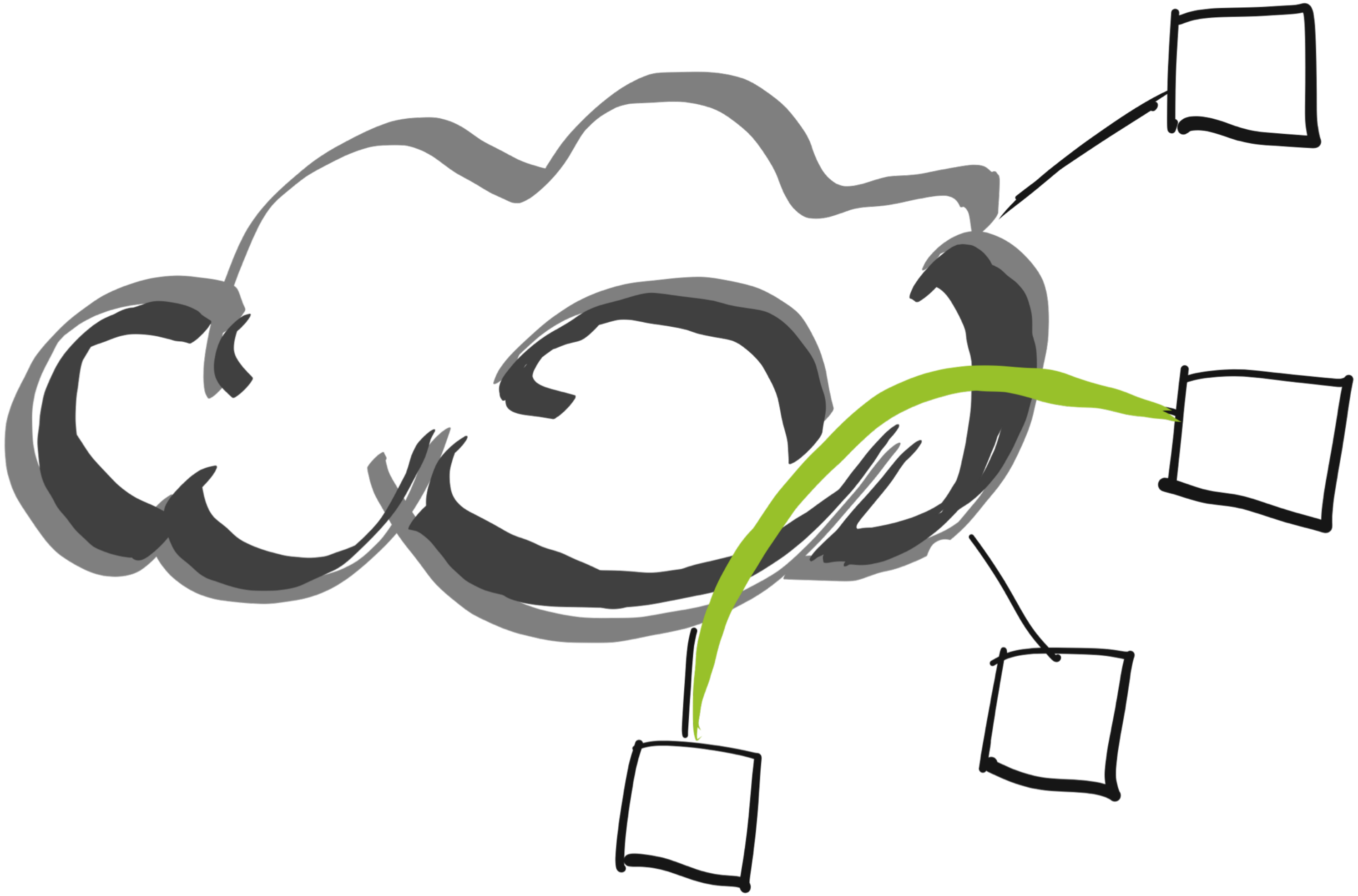
Computer Network Defense

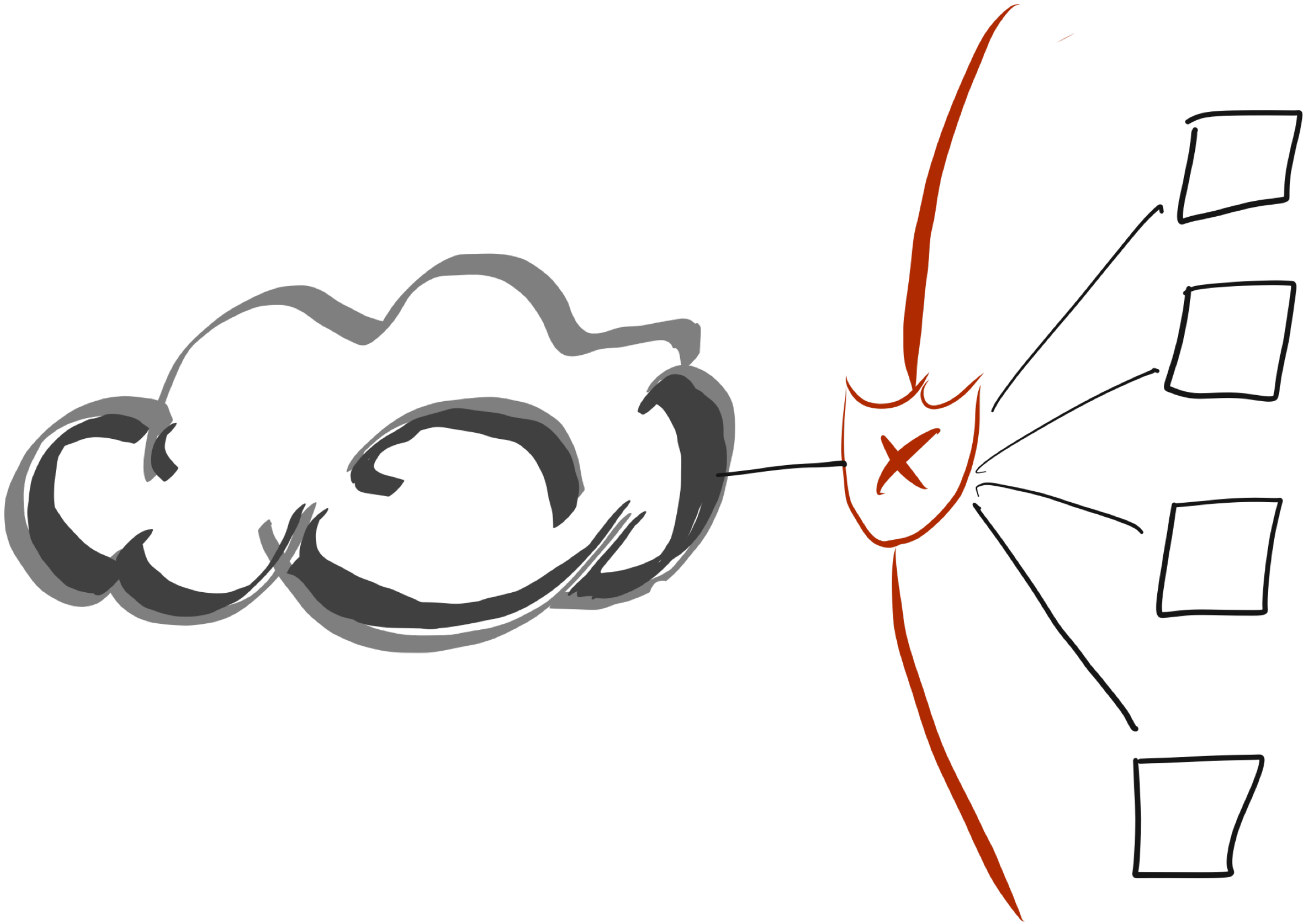
- **Protect** the network by focusing on securing systems and to prevent exploitation and intrusion from occurring by hardening network and computer systems, vulnerability scanning and vulnerability management, risk assessments and risk management.
- **Detect** threats towards the network by focusing on detecting intrusions that are currently active or intrusions that were successful in the past, by monitoring systems, sensing attacks and issue alarms and warnings.
- **Respond** to threats in the network by focusing on responding to intrusions, isolating compromised assets, performing host and network forensics, malware analysis and reporting.
- **Sustain** the operational capabilities of CND by focusing on managing people, processes, and technologies in the forms of capability development, systems implementation, staffing, policies development, and routines writing.

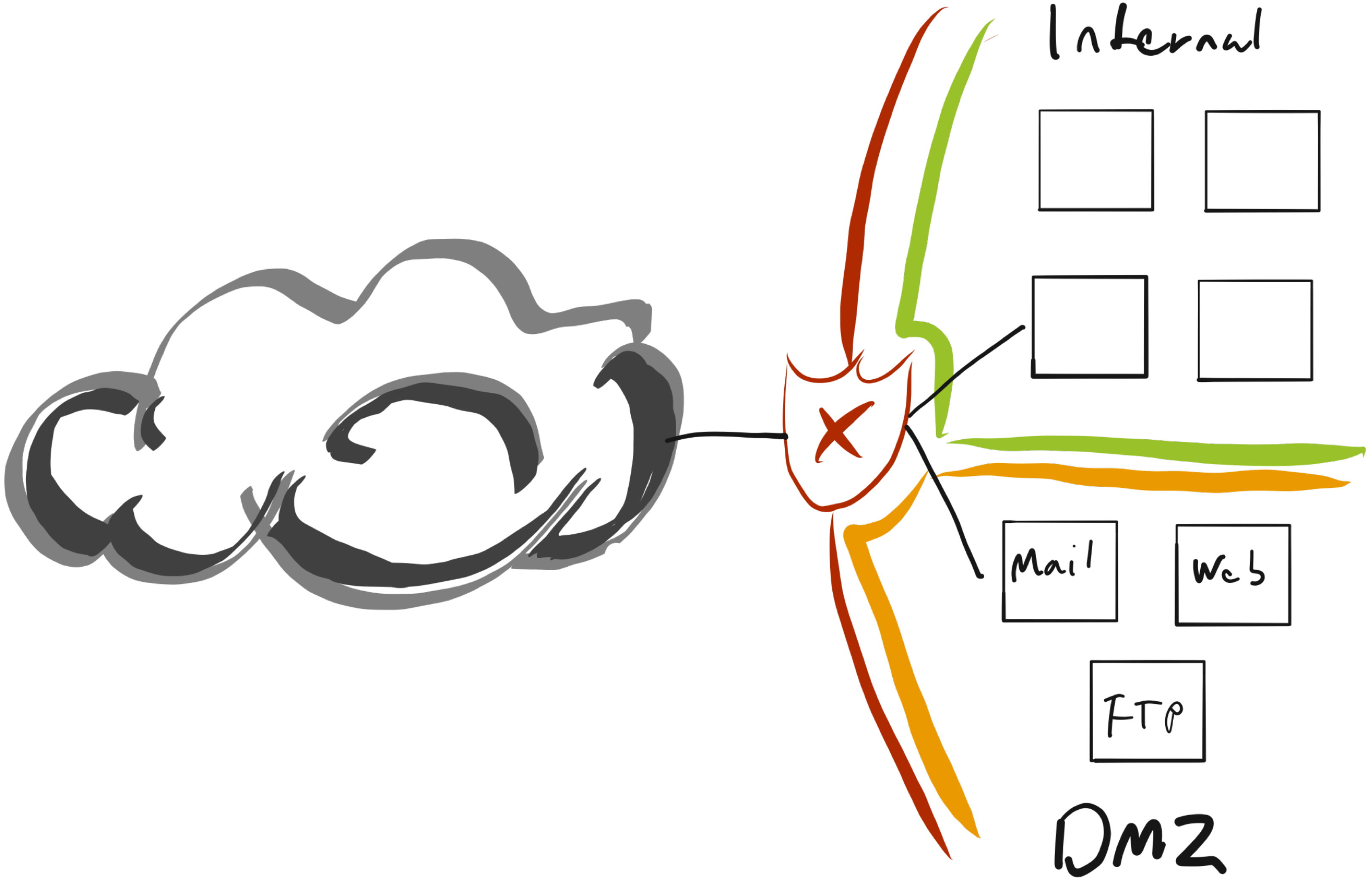
Problemspace: Defense Complexity

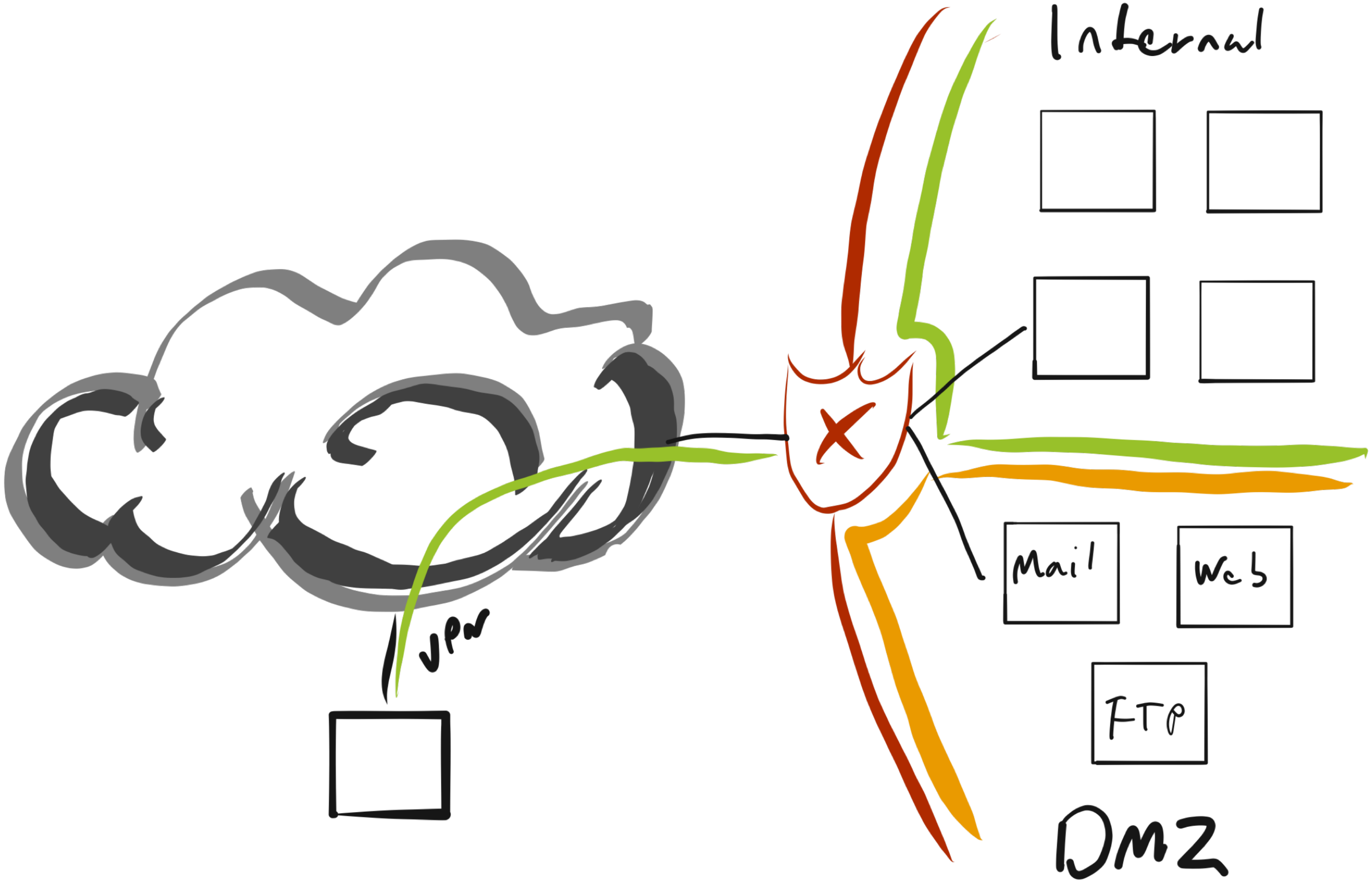
Complexity is the enemy of security.

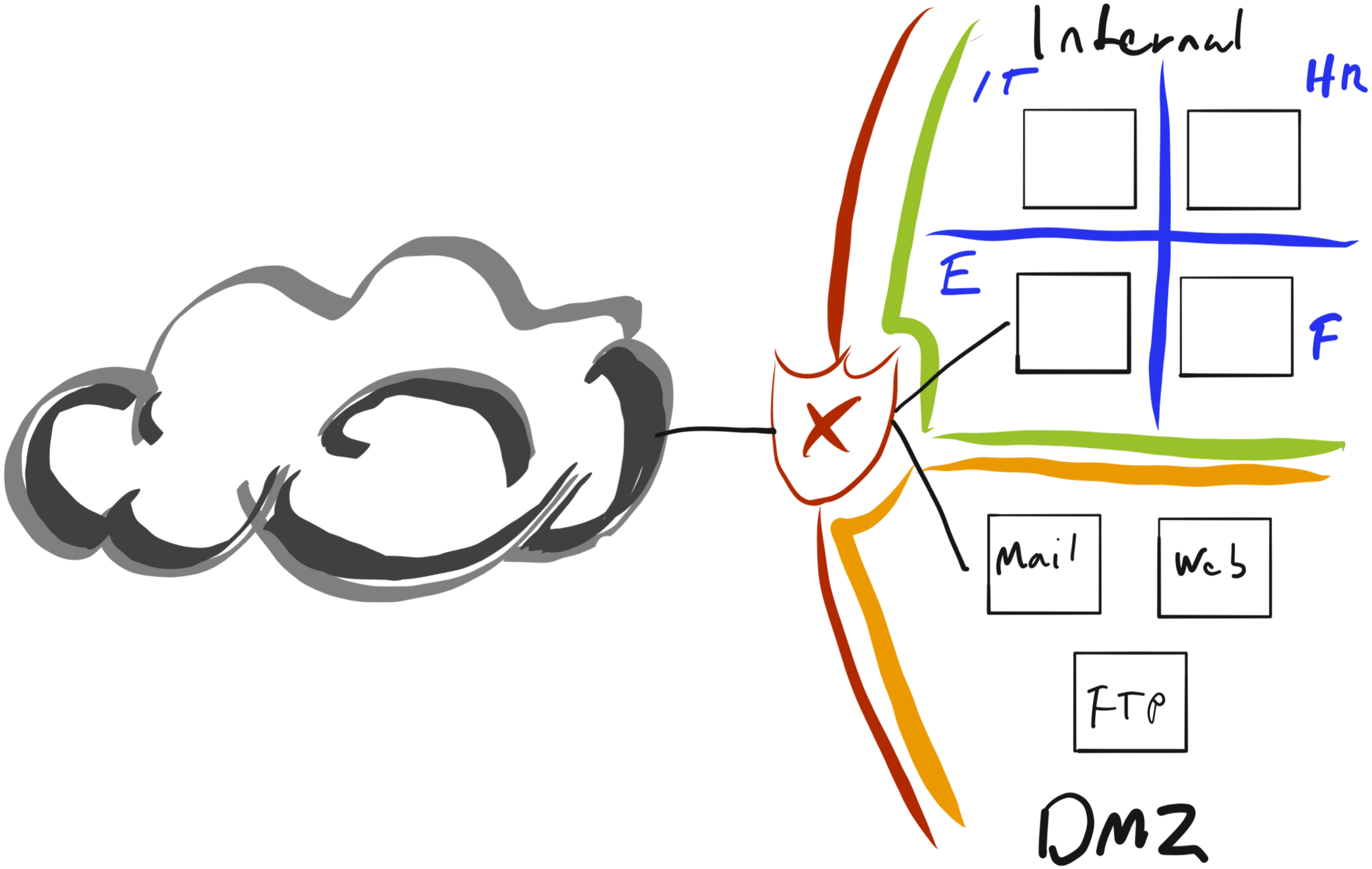


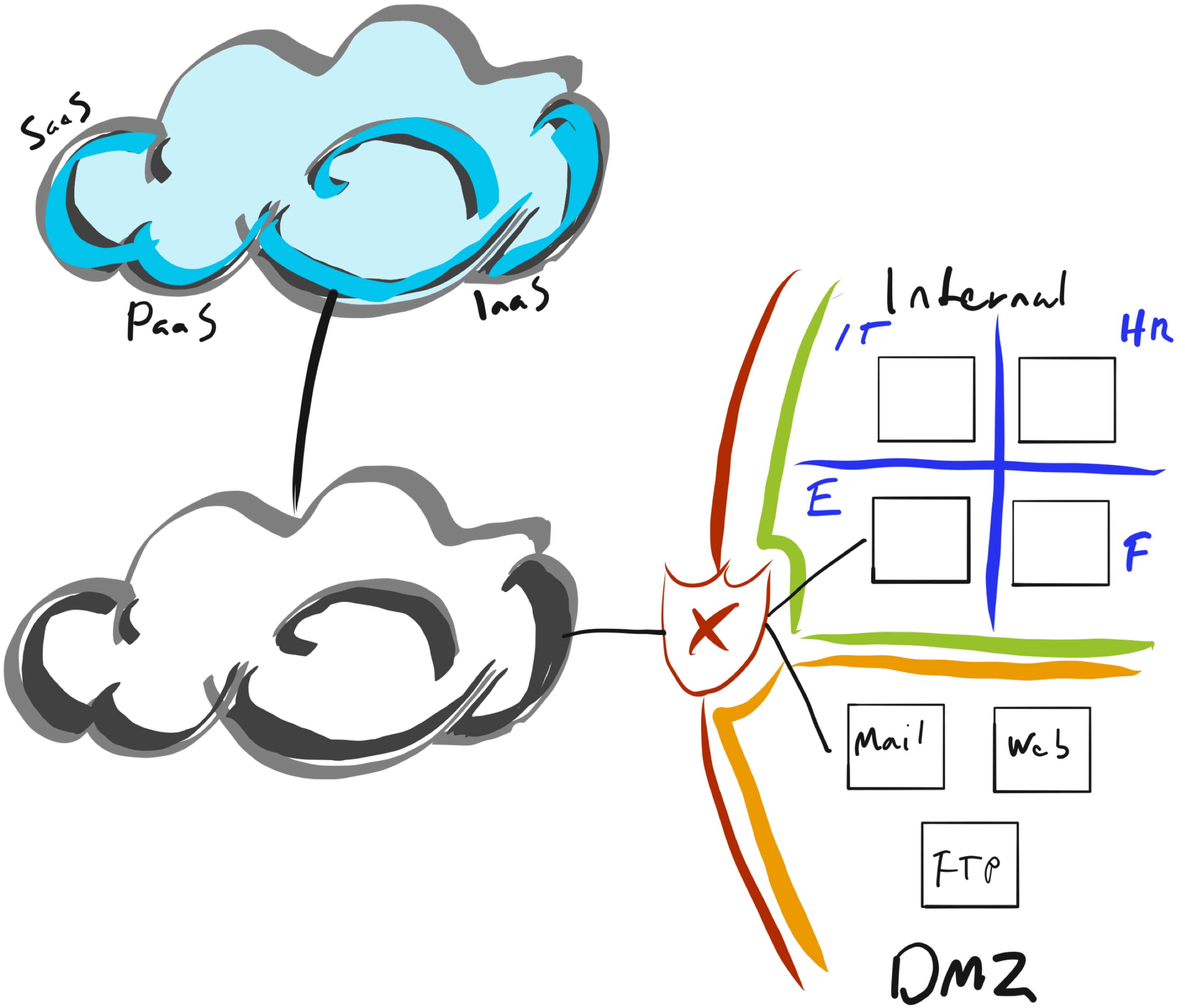


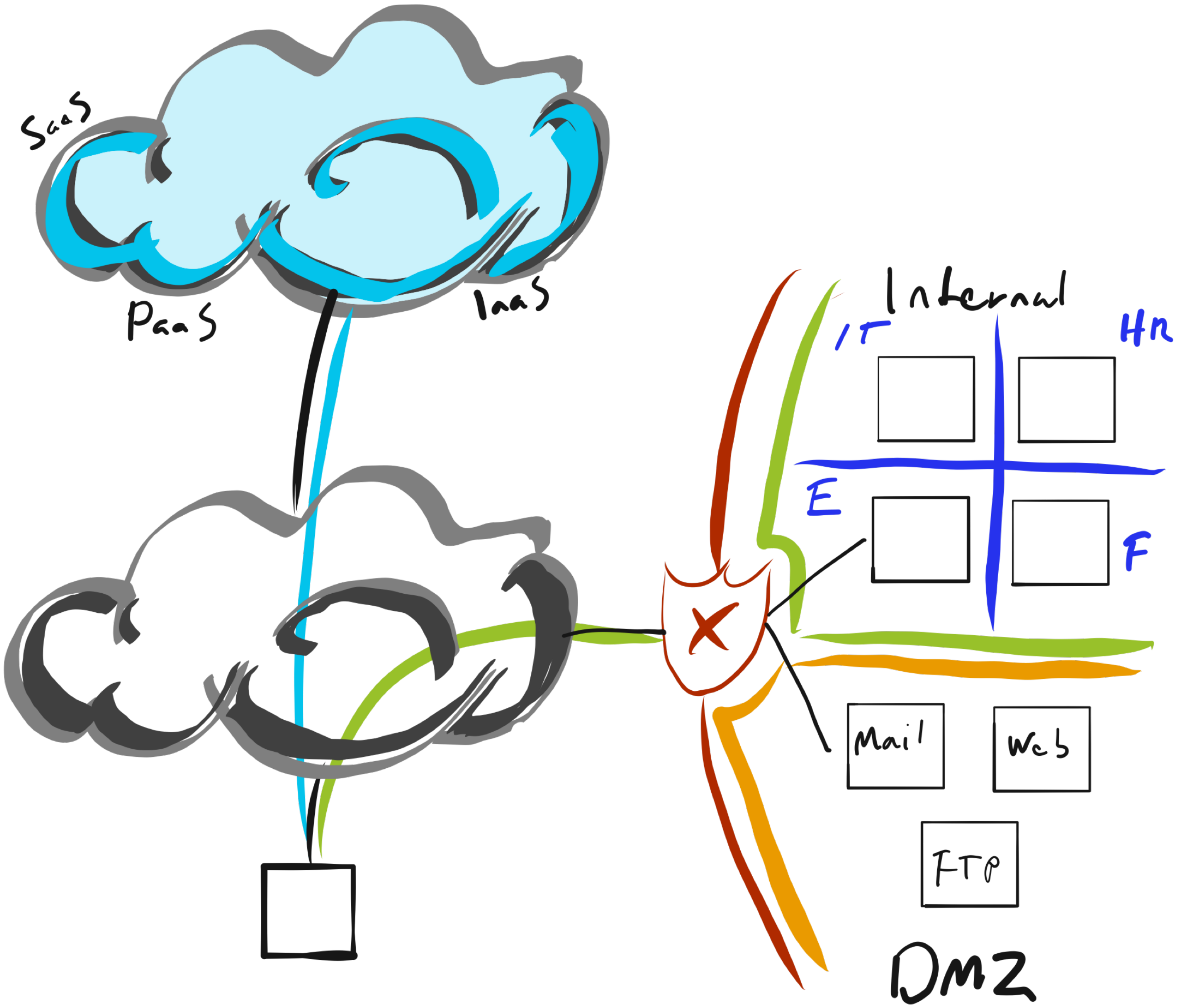


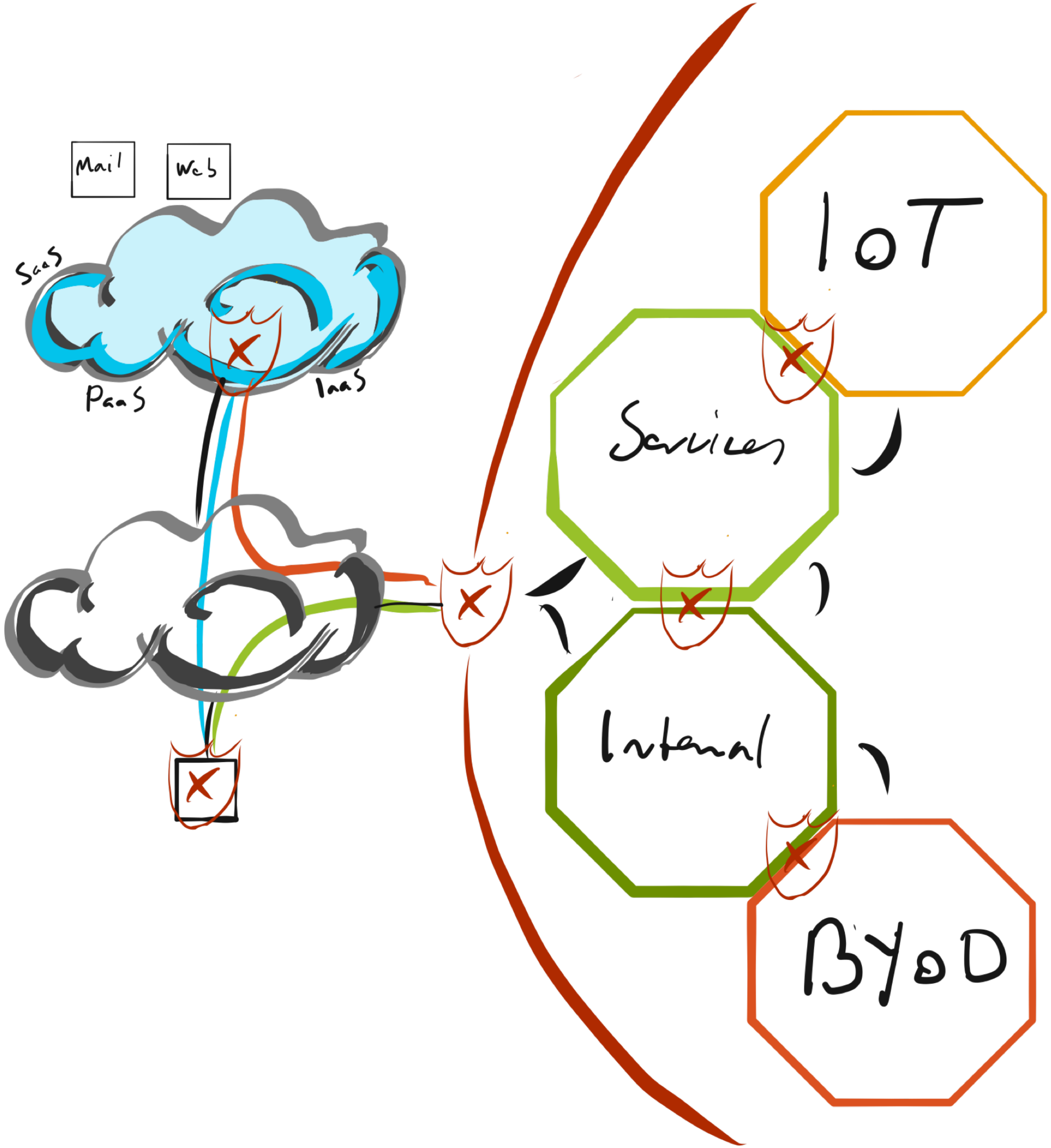

Internal
Mail
Web
FTP
DMZ


Internal
VPN
Mail
Web
FTP
DMZ


Internal
IT
HR
E
F
Mail
Web
FTP
DMZ


SaaS
PaaS
IaaS
Internal
IT
HR
E
F
Mail
Web
FTP
DMZ


SaaS
PaaS
IaaS
Internal
IT
HR
E
F
Mail
Web
FTP
DMZ


Mail
Web
SaaS
PaaS
IaaS
IoT
Services
Internal
ByoD

Network defense requirements

Protect: The first line of defense.

Four fundamental questions to ask before thinking about computer network defense:

- What are we protecting?
- What are the threats?
- How do we detect the threats?
- How do we repond to threats?

Bollinger, Jeff; Enright, Brandon; Valites, Matthew. Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan

Threats

1. Opportunistic attackers
2. Targeted attackers
3. Insider threats
4. Trusted insider threats
5. State-level actor

Capability of threats:

- Knowledge
- Infrastructure
- Resources / Funding
- Tool sophistication

Defendable IT architecure

A defendable computer network is a network that is:

- Monitored – Detect what is on the network
- Inventoried – Know what is on the network
- Controlled – Implement security controls
- Claimed – Policies and ownership of assets
- Minimized – Attack surface reduction
- Assessed – Risk, Threat and Vuln. -assessments
- Current – IT service management

https://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html

Information Security Management System

- An systematic approach to risk, vulnerabilities, threats and Information Security
  - Incident reporting
  - Incident response
  - Risk assessment
  - Threat assessement
  - Vulnerability assessment
- Well defined plans for incident response, disaster recovery and business contingency
- Asset value and context put into system
- Continuous improvement
- Priority, Classification and Rating
- Legal boundaries

Technology solves only 26% of current security challanges (Cisco Annual Threat report).

Vulnerability management

- Vulnerability feeds (CVE´s)
- Vendor PSIRT feeds
- Commercial vuln feeds
- Open community feeds
- Vulnerability scanning
- Vulnerability database
  - What is vulnerable on the network?
  - Where is vulnerable assets located?
  - How is it vulnerable?
  - Risk reducing control mechanisms?

Risk assessments

- Technical risk assessment
- Organisational risk assessment
- Business Impact Analysis (BIA)
- Penetration testing

Why?

- Identify organisational risks
- Identify process risks
- Identify system risks
- Identify component risk

Risk Management (1)

Fundamental goals of an information security risk management program:

- Improve the security posture of the organization
- Empower business units to identify and remediate risks
- Help prioritize remediation tasks
- Educate the organization regarding real threats and weaknesses
- Increase visibility and capability to track risks
- Improve the consistency of risk assessment approaches
- Establish a common formula for risk evaluations
- Meet audit, regulatory, and customer expectations

Wheeler, Evan. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up

Risk management (2)

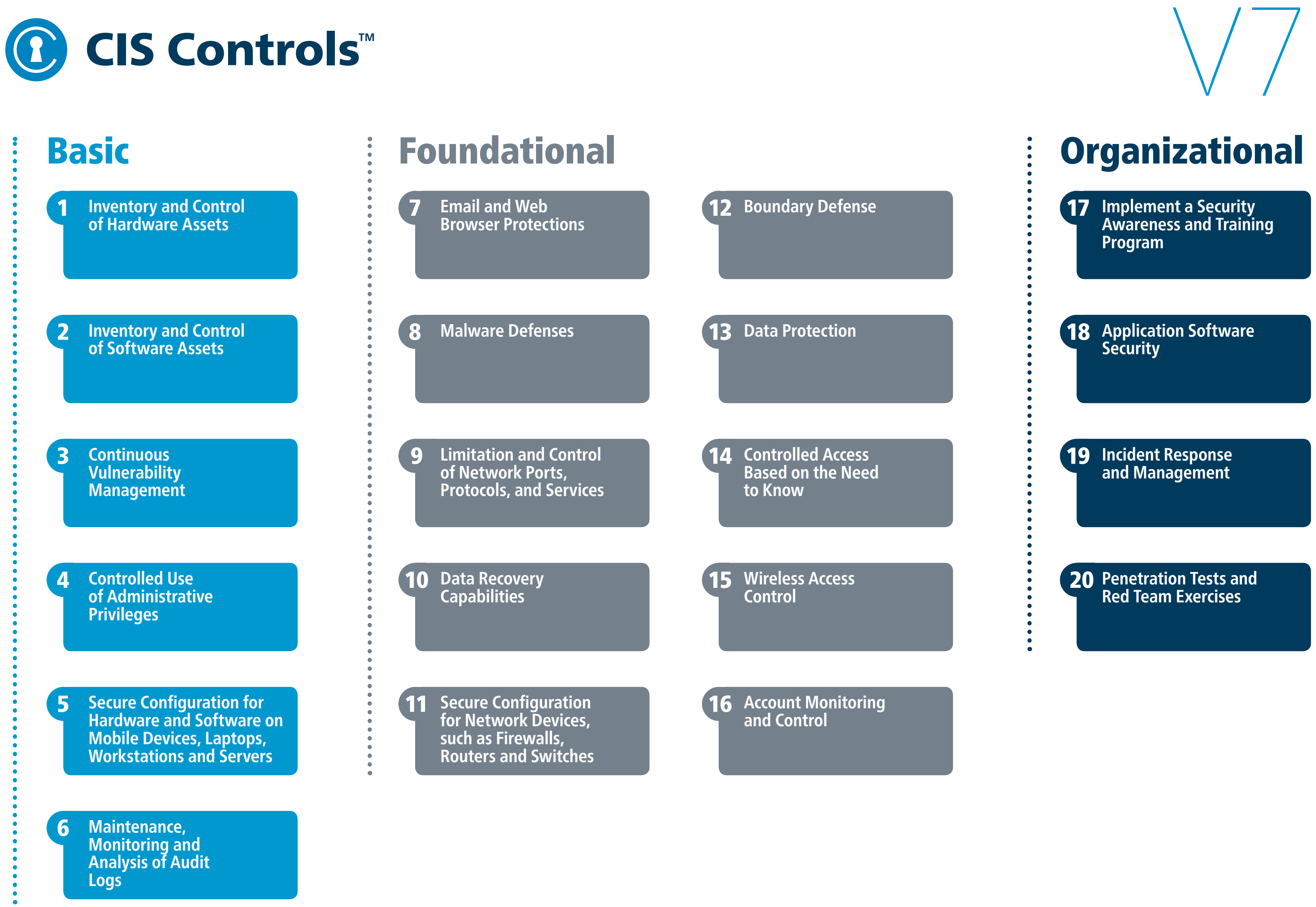
- Pre: Security policies and standards
- Information resources inventory
  - Asset inventory database
  - Configuration database
  - Customer Relation database
- Common risk formulae
- Enterprise risk committee
- Mapping risk domains to business objectives
- Risk tracking

Wheeler, Evan. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up

Risk Management (3)

- Asset management
- Business contingency
- Change management
- Outsourcing
- Privacy and data protection
- Physical or enviromental

Wheeler, Evan. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up



CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

https://www.cisecurity.org

Essential protection controls (1)

- Application whitelisting – to control the execution of unauthorised software
- Patching applications – to remediate known security vulnerabilities
- Configuring Microsoft Office macro settings – to block untrusted macros
- Application hardening – to protect against vulnerable functionality

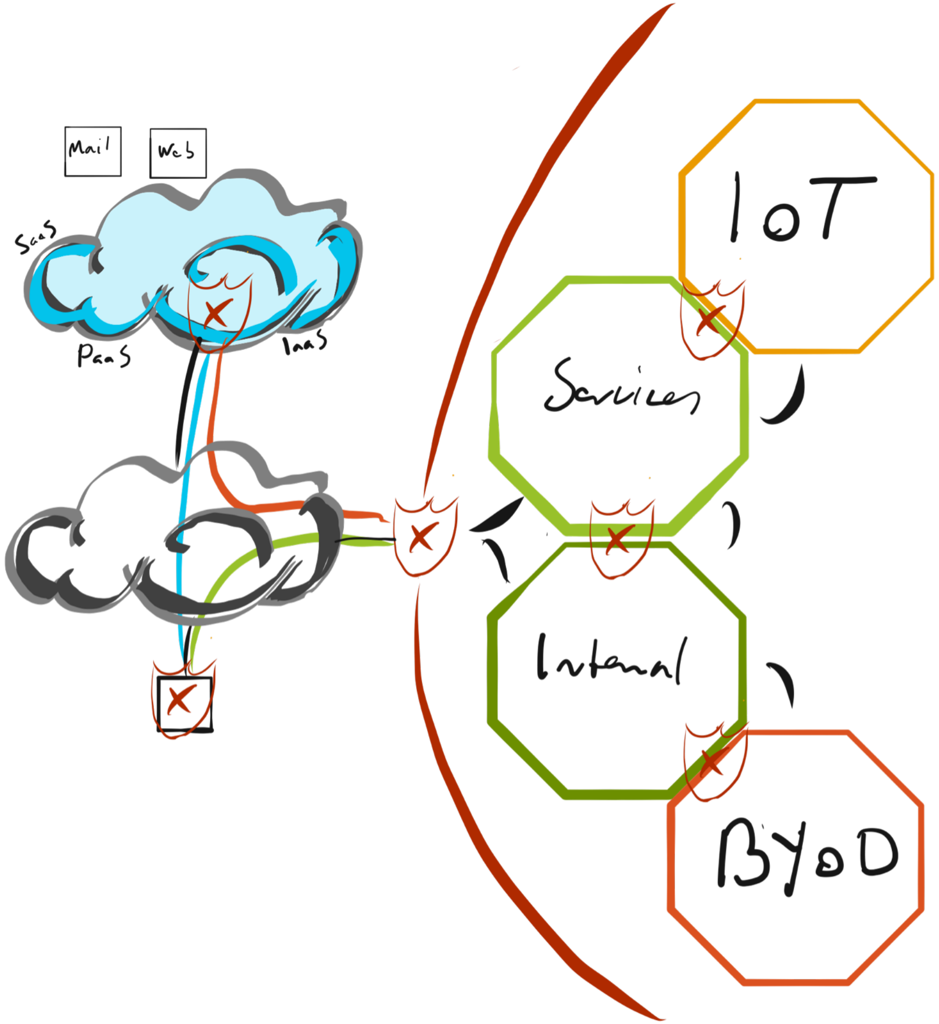
https://acsc.gov.au/infosec/mitigationstrategies.htm

Essential protection controls (2)

- Restricting administrative privileges – to limit powerful access to systems
- Patching operating systems – to remediate known security vulnerabilities
- Multi-factor authentication – to protect against risky activities
- Daily backups – to maintain the availability of critical data.

https://acsc.gov.au/infosec/mitigationstrategies.htm

KEEP
CALM
AND
PLAN,
DO, CHECK,
ACT!


Mail
Web
SaaS
PaaS
IaaS
IoT
Services
Internal
ByoD

Zero Trust Networks

1. The Network is **always** assumed to be hostile
2. External and internal threats are always present on the network, at all times.
3. Network locality is not sufficient for deciding trust in a network
4. Every user, device and network flow is authenticated and authorized, all the time.
5. Security policies must be dynamic and calculated based upon as much information as possible

Gilman, Evan. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media.

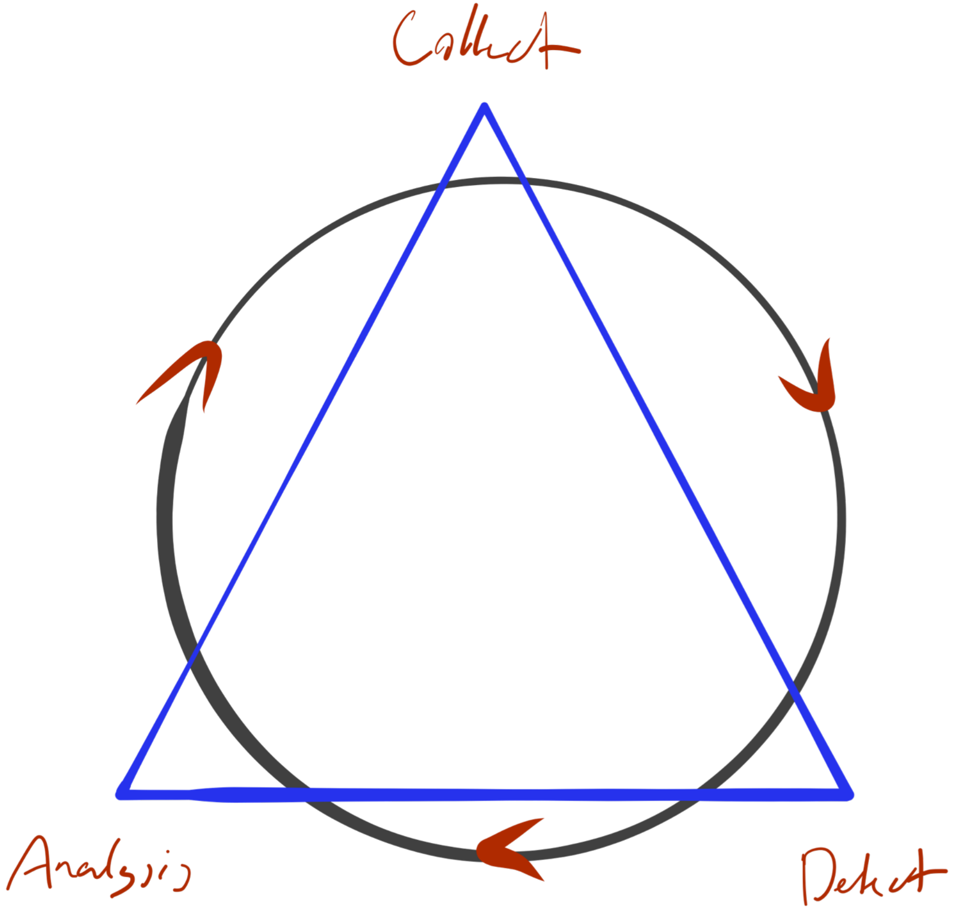
Network Security Monitoring

Detect: When protection fails.

Network Security Monitoring

- NSM is all about Indicators and Warnings
- NSM focus on:
  - the collection of data that describes the network environment to the greatest extent possible,
  - providing incident responders, security professionals, and forensic analysts with data for:
    - responding,
    - understanding,
    - recovering, and;
    - protecting org. assets.
- Collecting relevant information to the extent of technology, policy and law.
- Significantly Increase the likelihood of intrusion detection, as well as analyst understanding of intrusions

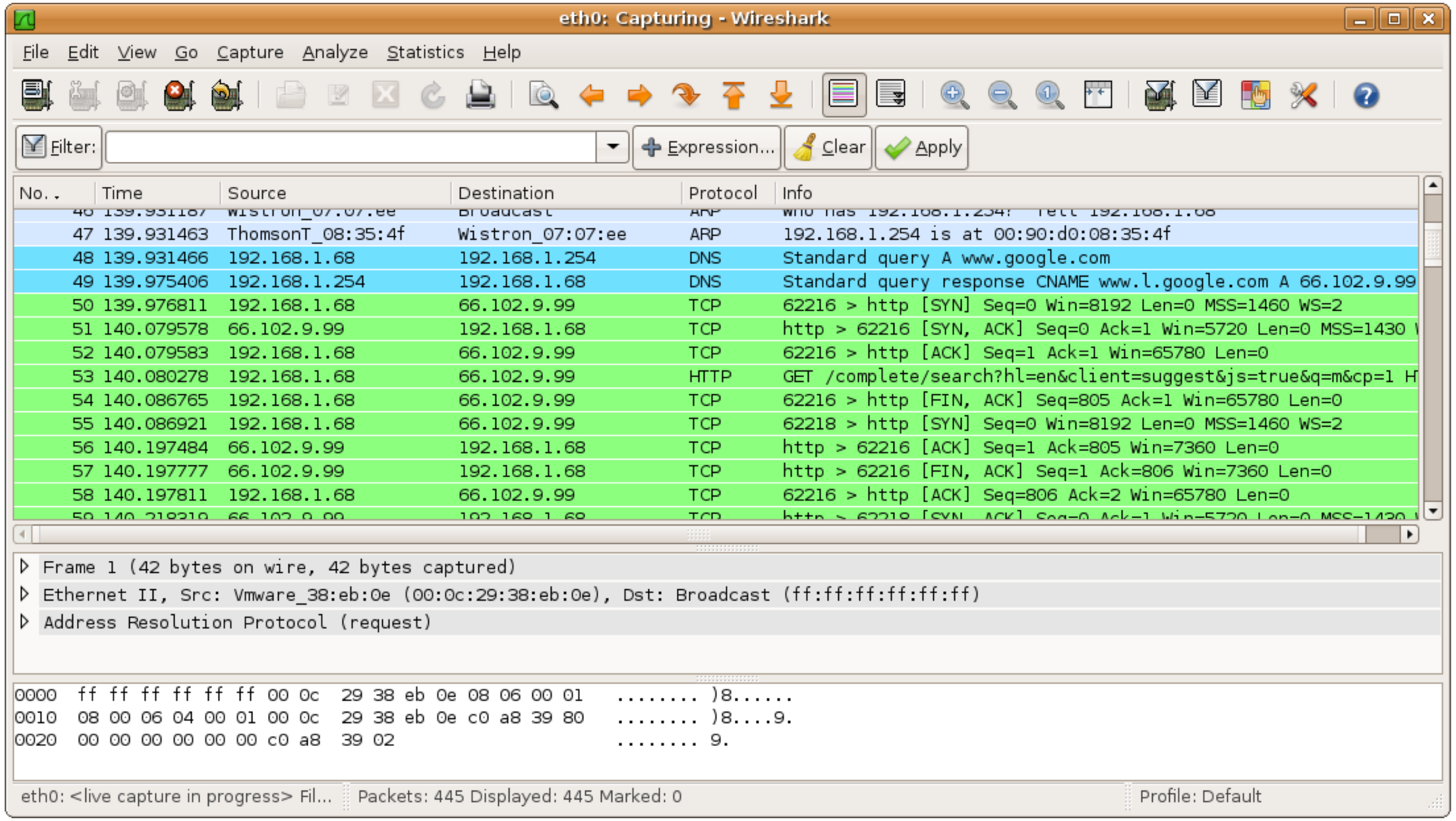
NSM has three phases:



NSM: Collection phase

- Full Packet Capture Data (Raw packet dump)
- Packet String Data (TLS, DNS, HTTP, SMB etc.)
- Session Data (Flow, Netflow, .1x)
- Statistical data
- Log data
- Alert data
- Metadata

Full packet capture (FPCD)


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source             Destination        Protocol  Info
 46 139.931187  Wistron_07:07:ee   Broadcast          ARP       Who has 192.168.1.254?  Tell 192.168.1.68
 47 139.931463  ThomsonT_08:35:4f  Wistron_07:07:ee   ARP       192.168.1.254 is at 00:90:d0:08:35:4f
 48 139.931466  192.168.1.68       192.168.1.254      DNS       Standard query A www.google.com
 49 139.975406  192.168.1.254      192.168.1.68       DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
 50 139.976811  192.168.1.68       66.102.9.99        TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
 51 140.079578  66.102.9.99        192.168.1.68       TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 \
 52 140.079583  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
 53 140.080278  192.168.1.68       66.102.9.99        HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
 54 140.086765  192.168.1.68       66.102.9.99        TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
 55 140.086921  192.168.1.68       66.102.9.99        TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
 56 140.197484  66.102.9.99        192.168.1.68       TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
 57 140.197777  66.102.9.99        192.168.1.68       TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
 58 140.197811  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
 59 140.218319  66.102.9.99        192.168.1.68       TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 \
```

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

eth0: <live capture in progress> Fil...

Packets: 445 Displayed: 445 Marked: 0

Profile: Default

Packet String Data

- Transaction data without the payload, can be extracted from FPCD
- Less space, longer retention
- Examples:
  - HTTP headers
  - FTP Headers
  - TLS Headers
  - SSH headers
  - SMB Headers
  - DNS (Query / Reponse)

Session data

- In short: All types of flows (NetFlow, sFlow, Flow)
- Transaction log of all communications on the network
- On busy networks, require quite a lot of storage for retention
- Timeline analysis

Statistical data

- Derived from:
  - Collection,
  - Organization,
  - Analysis,
  - Interpreted, and;
  - Presentation of existing data
- Vital for anomaly detection
- Vital for detection on large networks

Log data

- ***Informational*** **log** messages are designed to let administrators and users know that some benign event has occurred in the system.
- ***Debug*** **log** messages are designed to provide software developers and system administrators with information about the internal states of a piece of software or hardware so that problems can be identified and troubleshooted.
- ***Warning*** **log** messages are designed to notify system administrators about problems in the system which are not severe enough to affect system operation.
- ***Error*** **log** messages inform system administrators that something is wrong somewhere in the system and it is negatively affecting the operation.
- ***Alert*** **log** messages are notifying the administrator that something interesting.

Alert Data

- Is produced by a tool, based either upon signatures or computed anomaly detection.

Metadata: data about data

- Log data by itself give very little meaning and value
- Metadata provides context and understanding
- Context enrichment of alerts and logs
- **Context is key**

NSM: Detection phase

- Signature-based detection
  - Still very effective
  - Cheap but «expensive»
- Anomaly-based detection
  - Less effective
  - Expensive, but finds unknown threats
- Specification-based detection
  - Effective, but hard to implement
  - Suitable for IoT/OT
- **Hybrid-detection**

Defense in depth

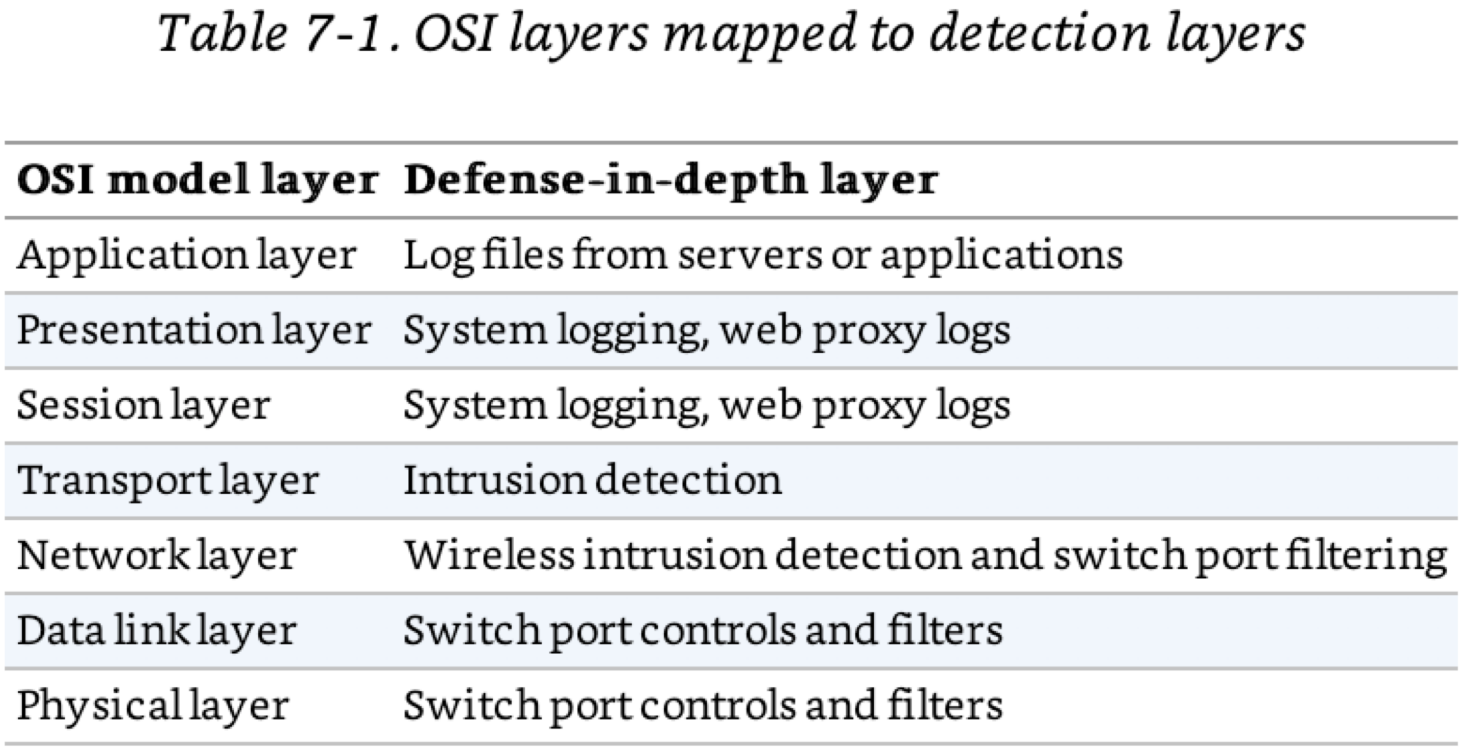


Table 7-1. OSI layers mapped to detection layers

OSI model layer	Defense-in-depth layer
Application layer	Log files from servers or applications
Presentation layer	System logging, web proxy logs
Session layer	System logging, web proxy logs
Transport layer	Intrusion detection
Network layer	Wireless intrusion detection and switch port filtering
Data link layer	Switch port controls and filters
Physical layer	Switch port controls and filters

Bollinger, Jeff; Enright, Brandon; Valites, Matthew. Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan

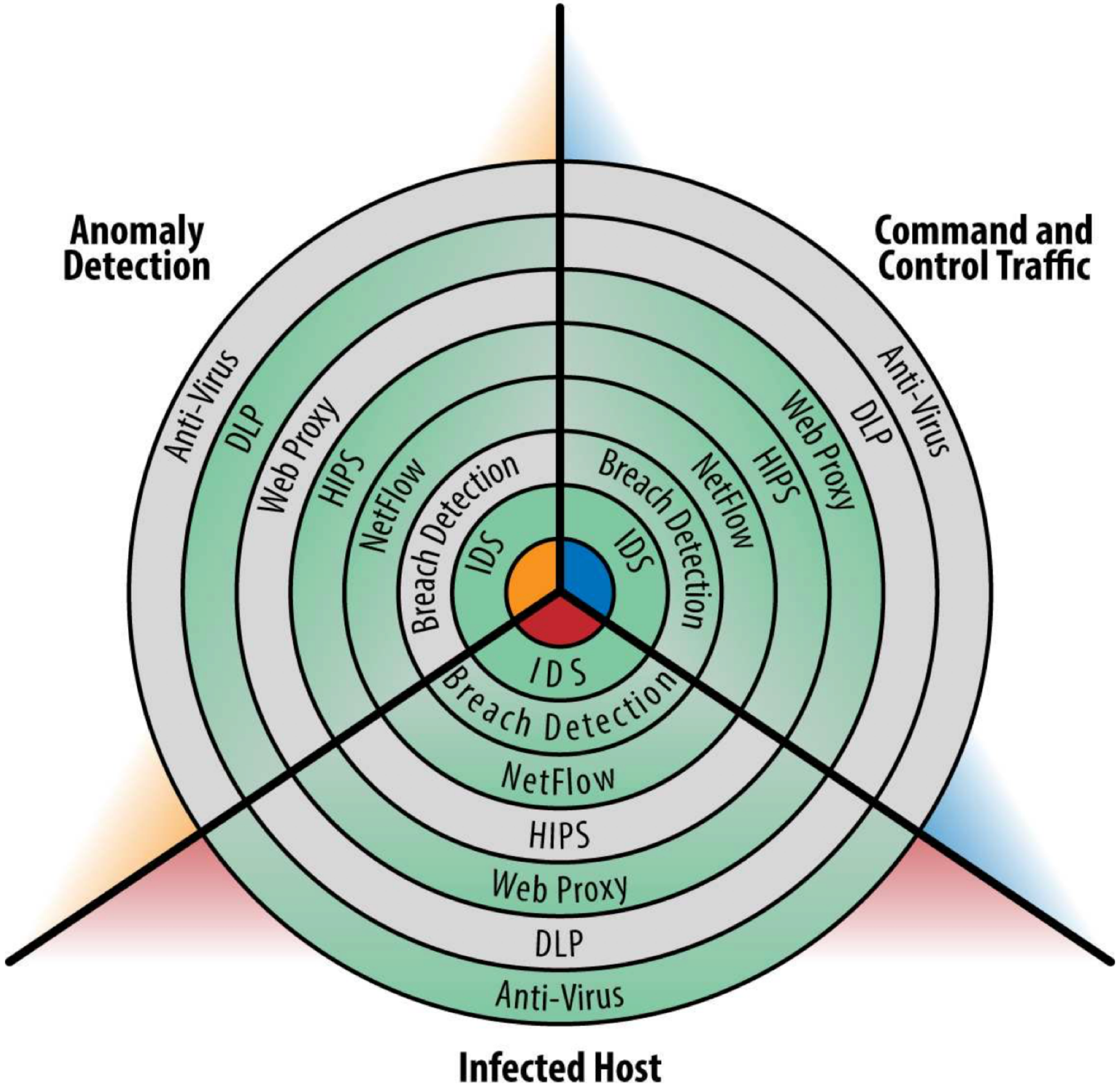


Figure 7-6. Sample overlay of threats per detection tool

Bollinger, Jeff; Enright, Brandon; Valites, Matthew. Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan

Cyber Threat Intelligence (1)

- *"the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations"* - ***US DoD***

- *"Evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard of assets that can be used to inform decisions regarding the subject's response to that menace or hazard"* - ***Rob McMillan, Gartner***

Cyber Threat Intelligence (2)

Cyber Threat Intelligence is not:

- A feed of bad IP´s
- A feed of bad domains
- A feed of hashes

Cyber Threat Intelligence is:

- Knowledge
- Context
- Interpretation
- Understanding

Cyber Threat Intelligence (3)

Three levels of CTI:

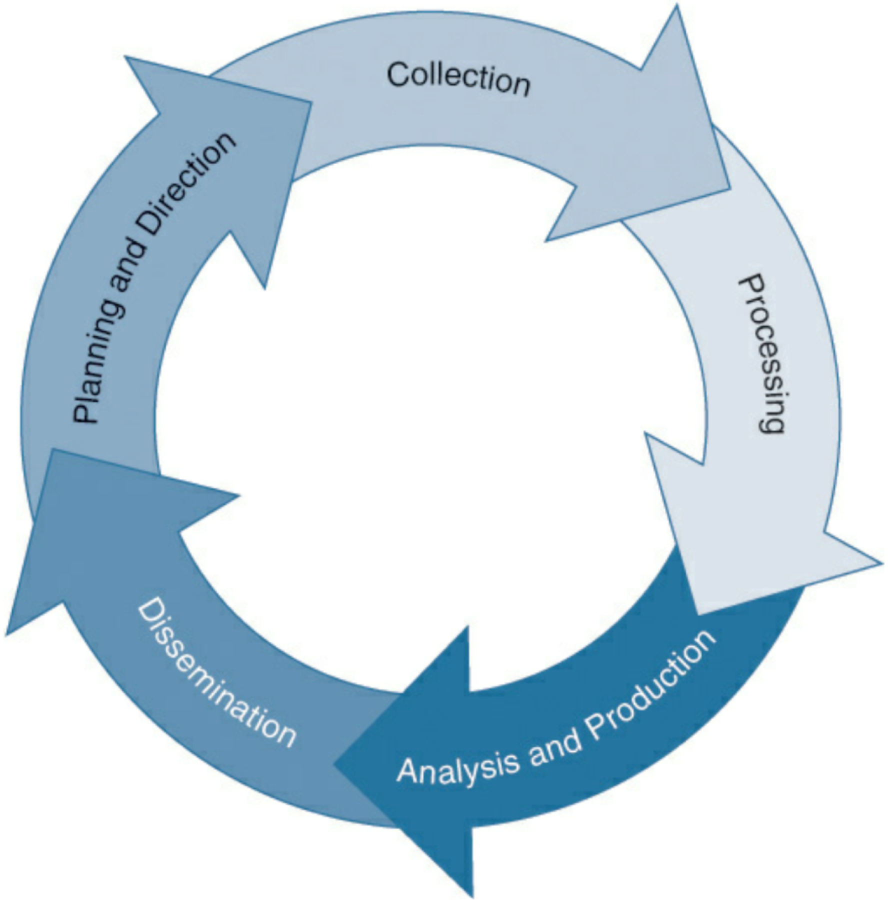
- Strategic intelligence (Who? Why? and Where?)
- Tactical Intelligence (What? When?)
- Operational Intelligence (How?)

Two types of indicators:

- Atomic Indicators
- Computed Indicators
- Behavior Indicators

[ERRATA]

Intelligence Cycle



Muniz, Joseph. Security Operations Center: Building, Operating, and Maintaining your SOC

The value of CTI

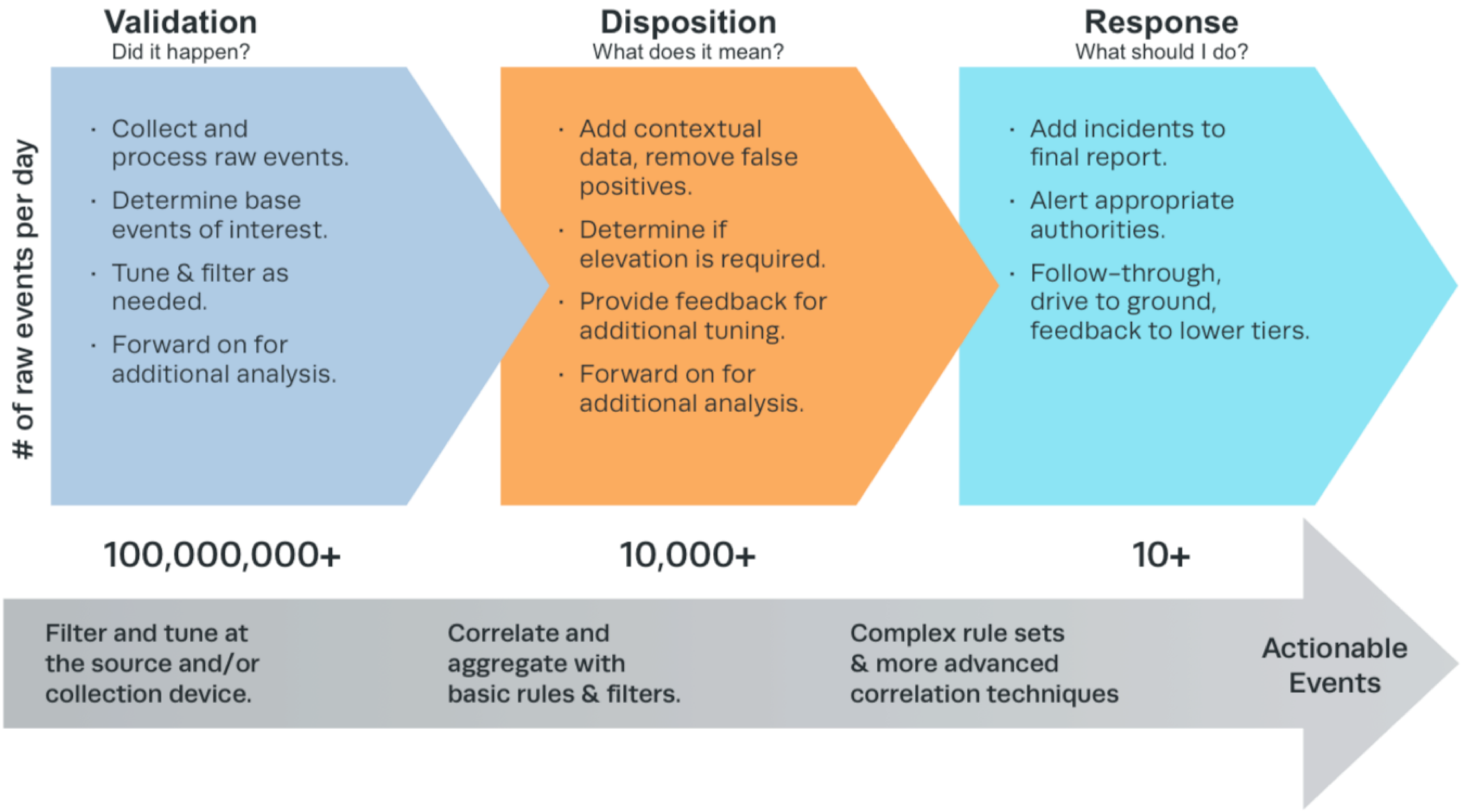
1. Breach identifications
2. Breach prevention
3. Fraud and theft minimization
4. Asset protection and risk minimization
5. User protection and risk minimization

Security Analytics and DFIR

Respond to threats.

NSM: Analysis phase

- A human analyst interprets the information from the detection stage to make a decision whether the warning is a real intrusion or a false positive alarm.
- This step often involves gathering information and investigative data from other sources, researching Open Source Intelligence related to the generated alert, and looking into the detection logic that produced the alert.
- Analysis is often the most time-consuming step in the NSM-cycle and might trigger the following tasks:
  - network packet analysis,
  - network forensics,
  - host forensics, and
  - malware analysis.



Validation
Did it happen?

- Collect and process raw events.
- Determine base events of interest.
- Tune & filter as needed.
- Forward on for additional analysis.

Disposition
What does it mean?

- Add contextual data, remove false positives.
- Determine if elevation is required.
- Provide feedback for additional tuning.
- Forward on for additional analysis.

Response
What should I do?

- Add incidents to final report.
- Alert appropriate authorities.
- Follow-through, drive to ground, feedback to lower tiers.

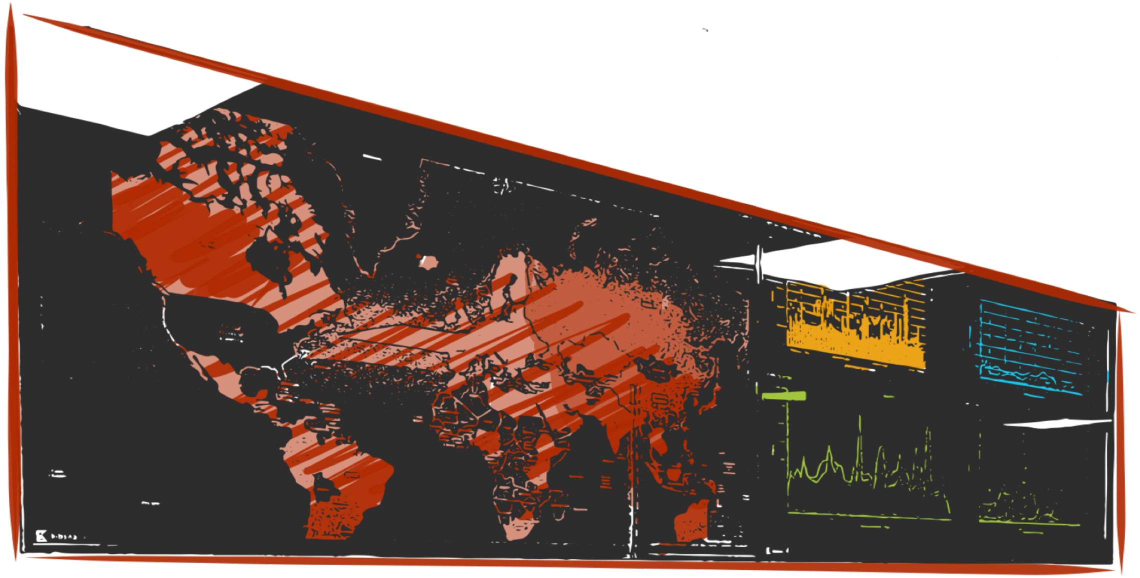
Filter and tune at the source and/or collection device.

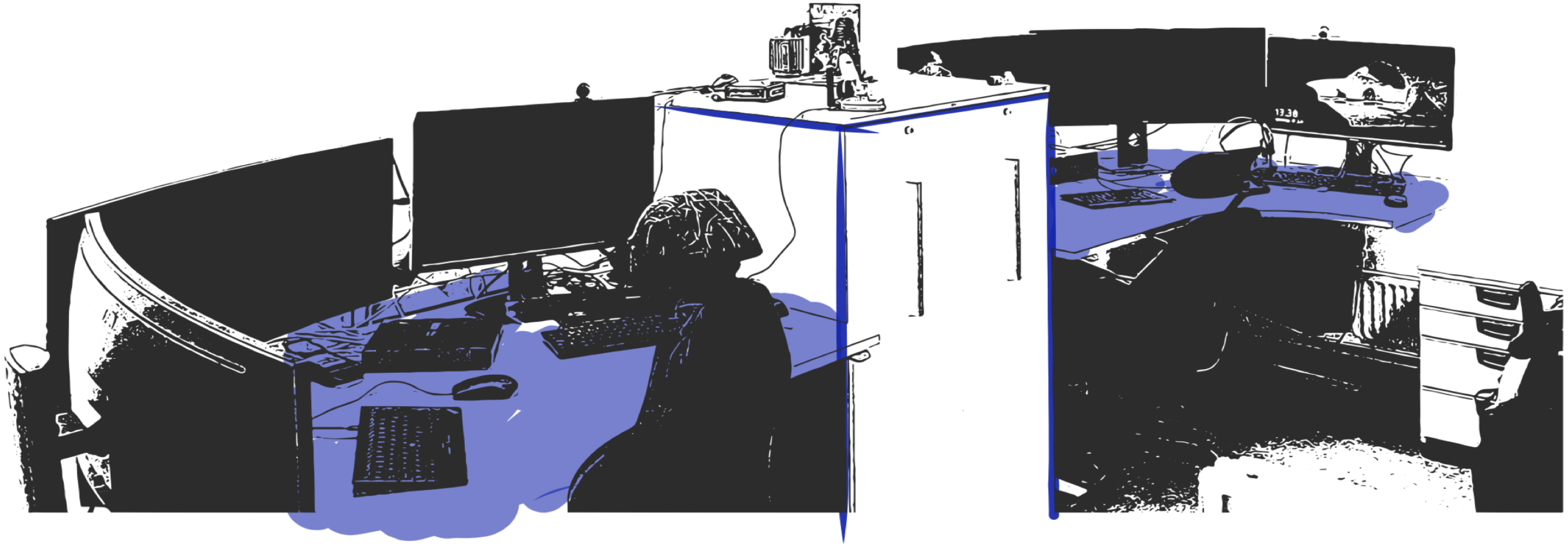
Correlate and aggregate with basic rules & filters.

Complex rule sets & more advanced correlation techniques

Figure 22. SIEM: Supporting the Event Life Cycle from Cradle to Grave

https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf





Incident Response

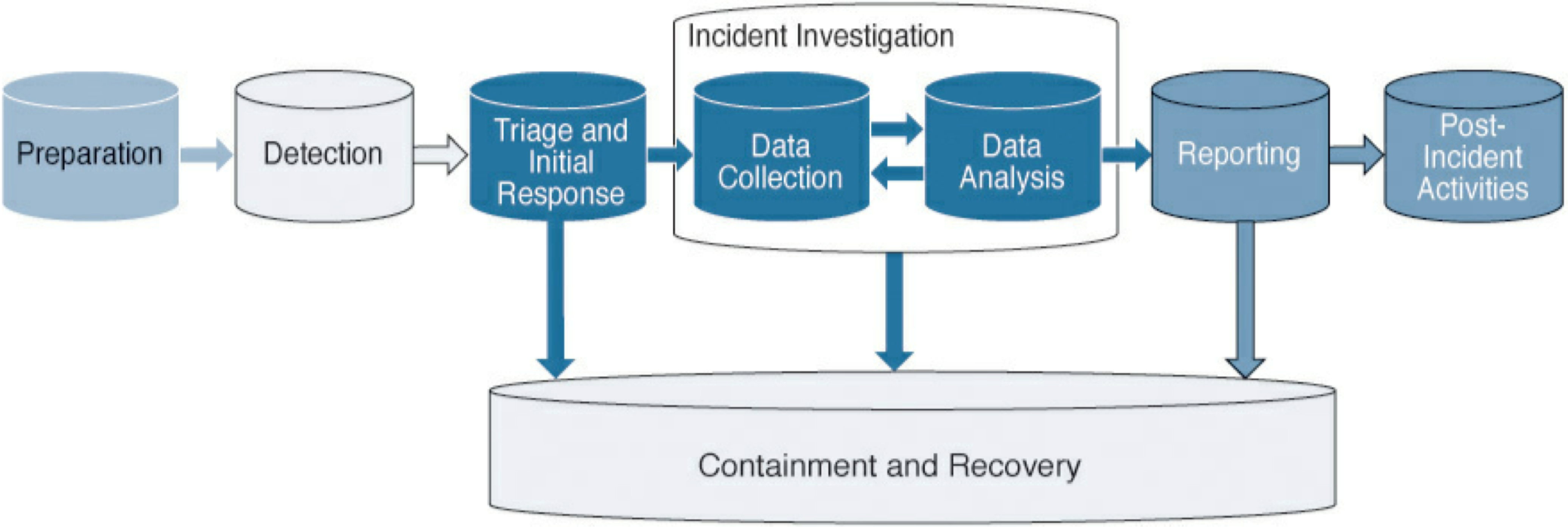


Figure 1-10 *Incident Response Timeline*

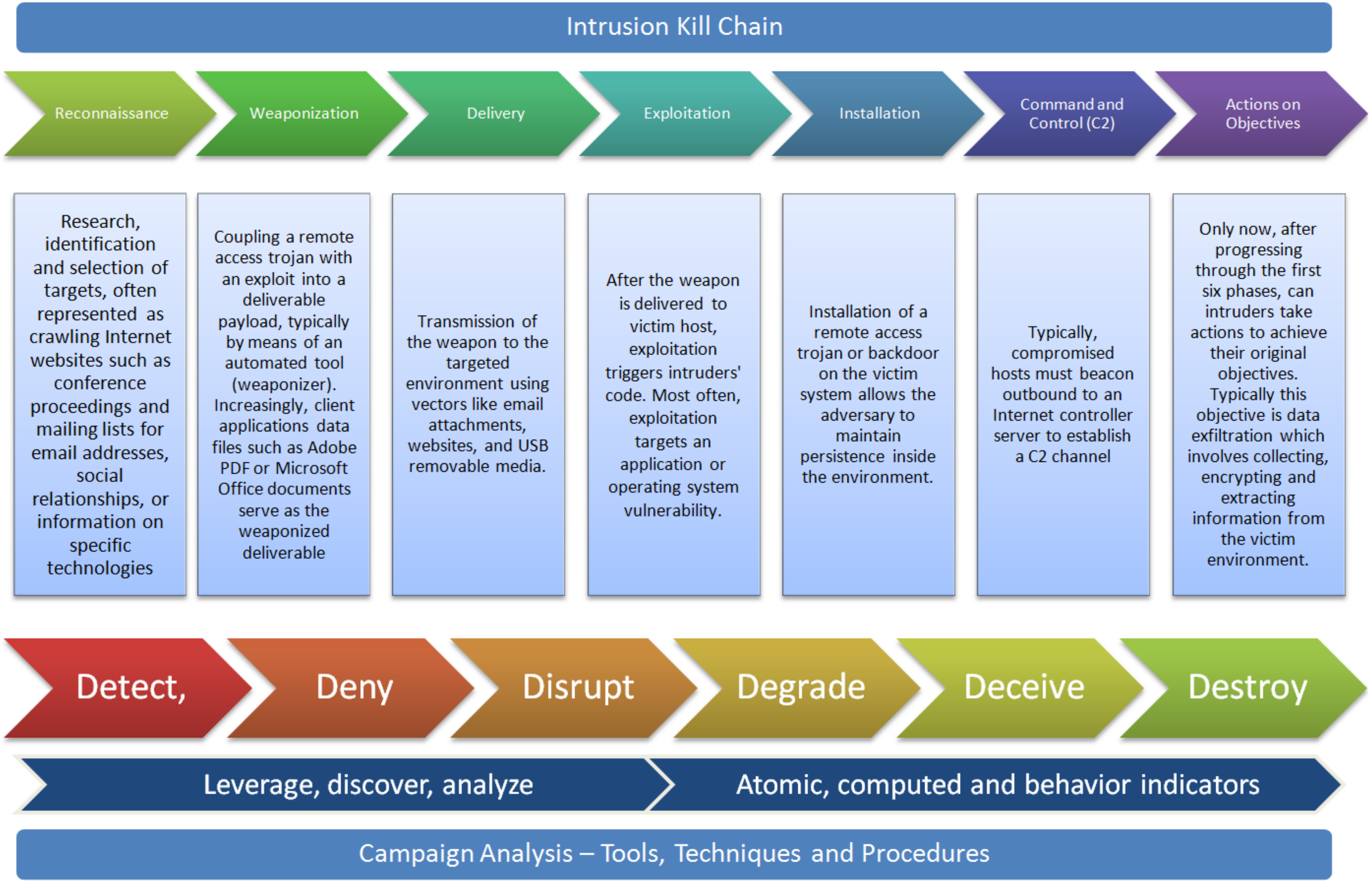
Security Operations Center: Building, Operating, and maintaining your SOC

Digital Forensics

- **Reactive DF:** *"Analythical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of digital media, which is digitally stored or encoded for evidentiary, and/ or root-cause analysis and the presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of incidents." -* Grobler, C., Louwrens, C., & Von Solms, S. H. 2010. A framework to guide the implementation of proactive digital forensics in organisations.

- **Proactive DF:** *"the proactive restructuring and defining of processes, procedures and technologies to create, collect, preserve and manage comprehensive digital evidence to facilitate a successful, cost effective investigation, with minimal disruption of business activities whilst demonstrating good corporate governance"* - Grobler, C., Louwrens, C., & Von Solms, S. H. 2010. A framework to guide the implementation of proactive digital forensics in organisations.

- **Active DF**: *"the ability of an organization to gather (identify, collect, and preserve) comprehensive digital evidence in a live environment to facilitate a successful investigation" -* Grobler, C., Louwrens, C., & von Solms, S. H. 2010. A multi-component view of digital forensics.



Intrusion Kill Chain

Reconnaissance: Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies

Weaponization: Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF or Microsoft Office documents serve as the weaponized deliverable

Delivery: Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removable media.

Exploitation: After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.

Installation: Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

Command and Control (C2): Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel

Actions on Objectives: Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment.

Detect, Deny Disrupt Degrade Deceive Destroy

Leverage, discover, analyze

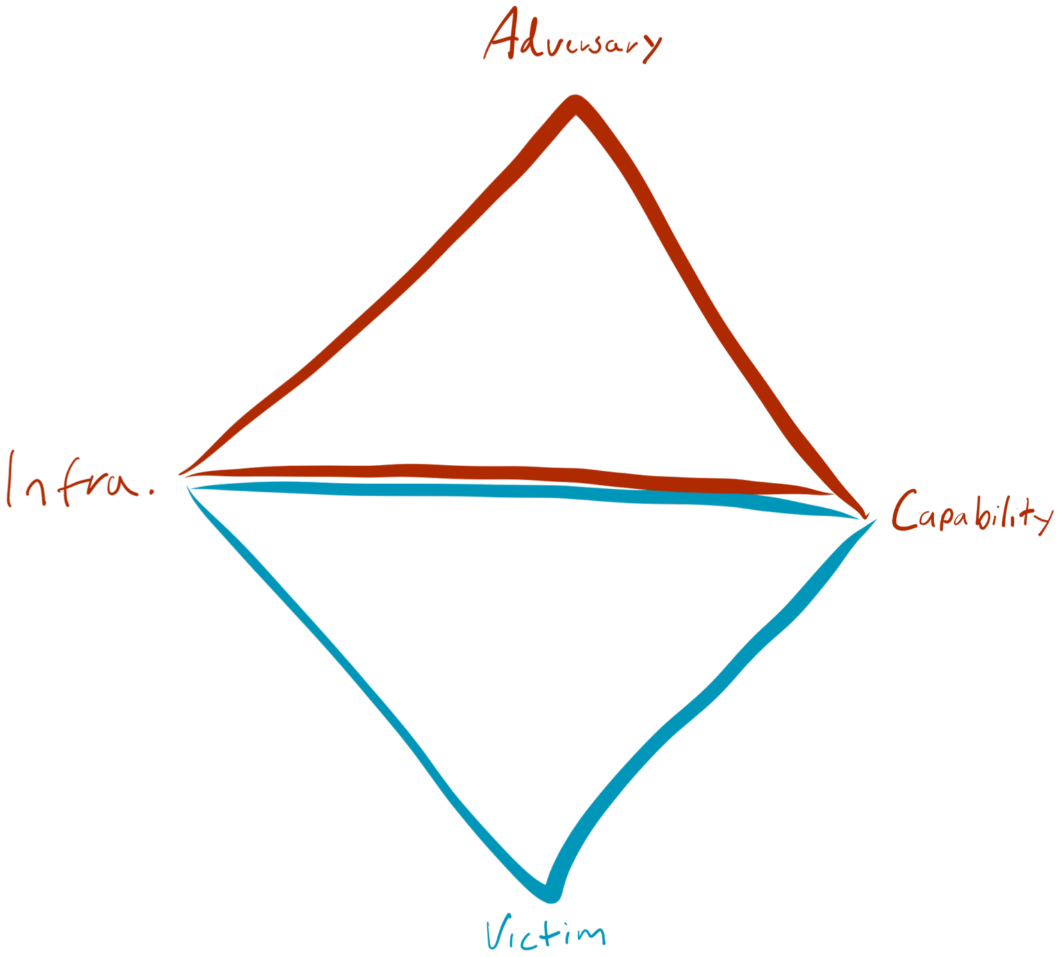
Atomic, computed and behavior indicators

Campaign Analysis – Tools, Techniques and Procedures

Original paper: Hutchins, E. M., Cloppert, M. J., & Amin, R. M. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.

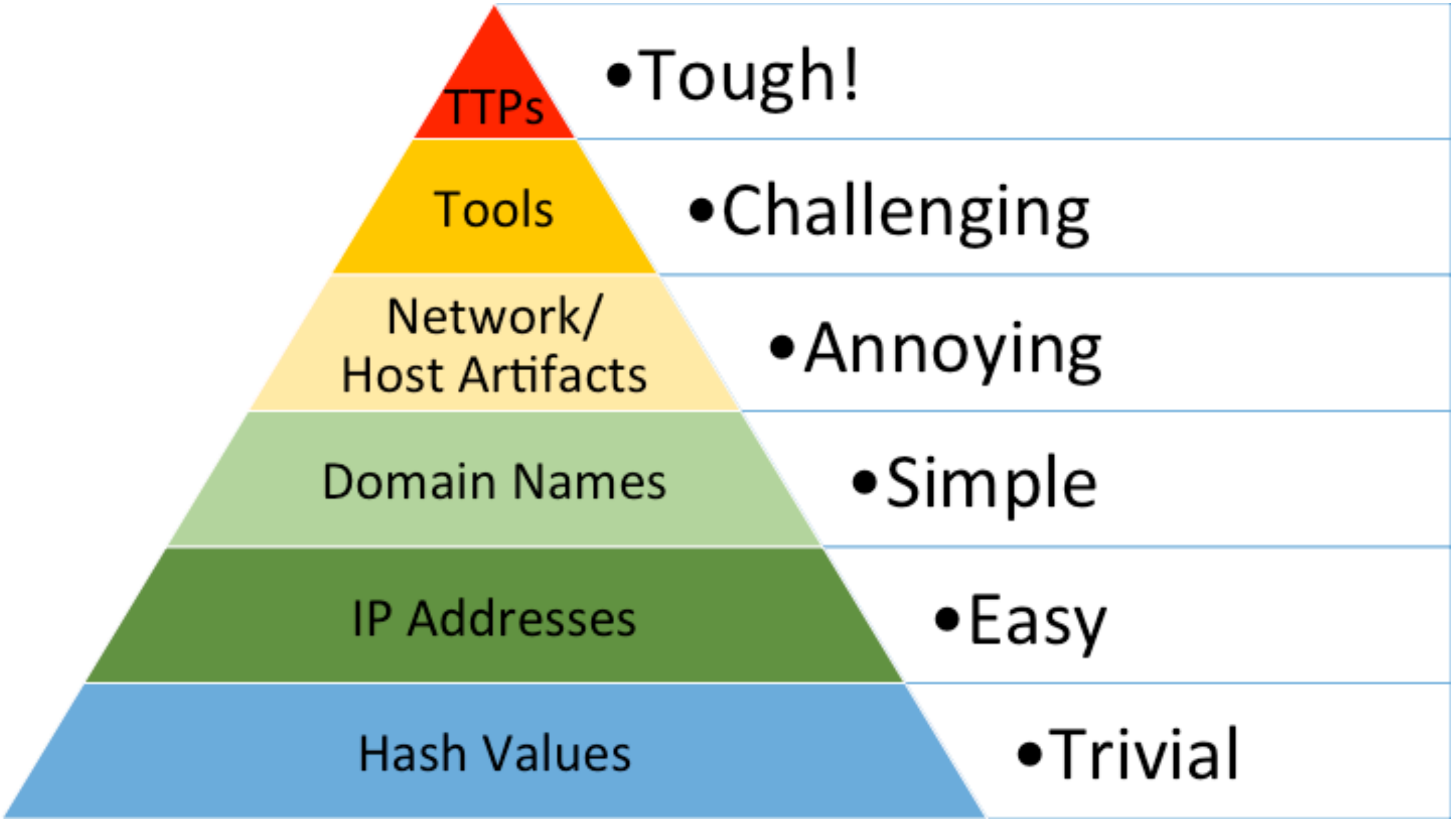
https://countuponsecurity.com/2014/08/29/intelligence-driven-incident-response/

Model: The Diamond model



http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Model: Pyramid of pain



TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Analyst cognitive biases

- **The paradox of expertise**: This cognitive bias can be experienced by an analyst that has been studying and working in the same area over many years. Thus, analyst can dismiss situational changes because they do not fit into the established patterns that have been observed over a long period of time. This leads to dismissing the event as not important or relevant because it is believed to be an error or a mistake.
- **Confirmation bias:** is a when an analyst looks more at, and value the indicators that support his/her hypothesis while dismissing or neglecting the importance and value of indicators that are contradicting his/her believes and hypothesis.
- **Coherence bias:** is when the analyst assumes that the group or an individual being studied have the same motivation and goals as the analyst himself. Thus, the analyst assigns the same values as he/she has to the subject, making himself unable to be objective, This results in overlooking vital information that in turn leads to the wrong conclusions of the finished intelligence.

Liska, Allan. *Building an Intelligence-Led Security Program*

Analyst Cognitive Bias 2

- **Hindsight bias:** often involves memory distortion, a phenomenon where memories are being altered to fit a new narrative. It can be expressed as "I know it all along" and "How could anyone miss this". Hindsight bias can be very damaging since it does not provide methodological analysis of past events in order to create new knowledge and learn from past mistakes.
- **Anchoring bias:** is when an analyst relies too much on one aspect of the collected data and weights a single indicator as more valuable then all the other indicators. This can often happen to the indicator an analyst get hold first during an investigation. This bias is often experienced by young or inexperienced analysts, but it is not limited to them.

Liska, Allan. *Building an Intelligence-Led Security Program*

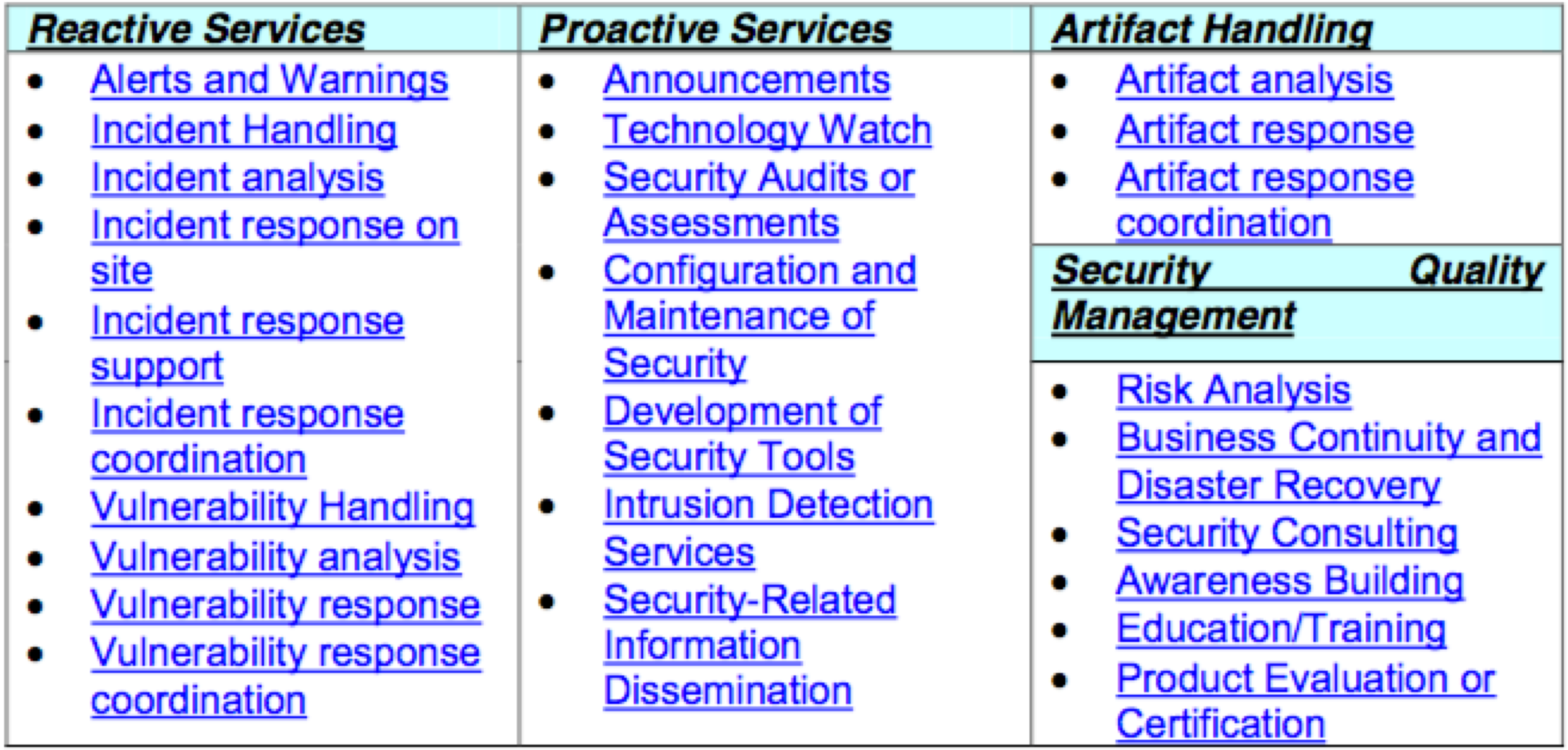
Security Operations

Sustain collect, detect and analysis cycle.

Security Operations (10 strategies)

1. Consolidate CND under one organization
2. Acheive balance between size and agility
3. Give SOC Authority to do its job
4. Do a few things well
5. Favor staff quality over quantity
6. Maximize the value of technology
7. Exercise discrimination over data that is collected
8. Protect the SOC
9. Produce and consume CTI
10. Repond to incidents

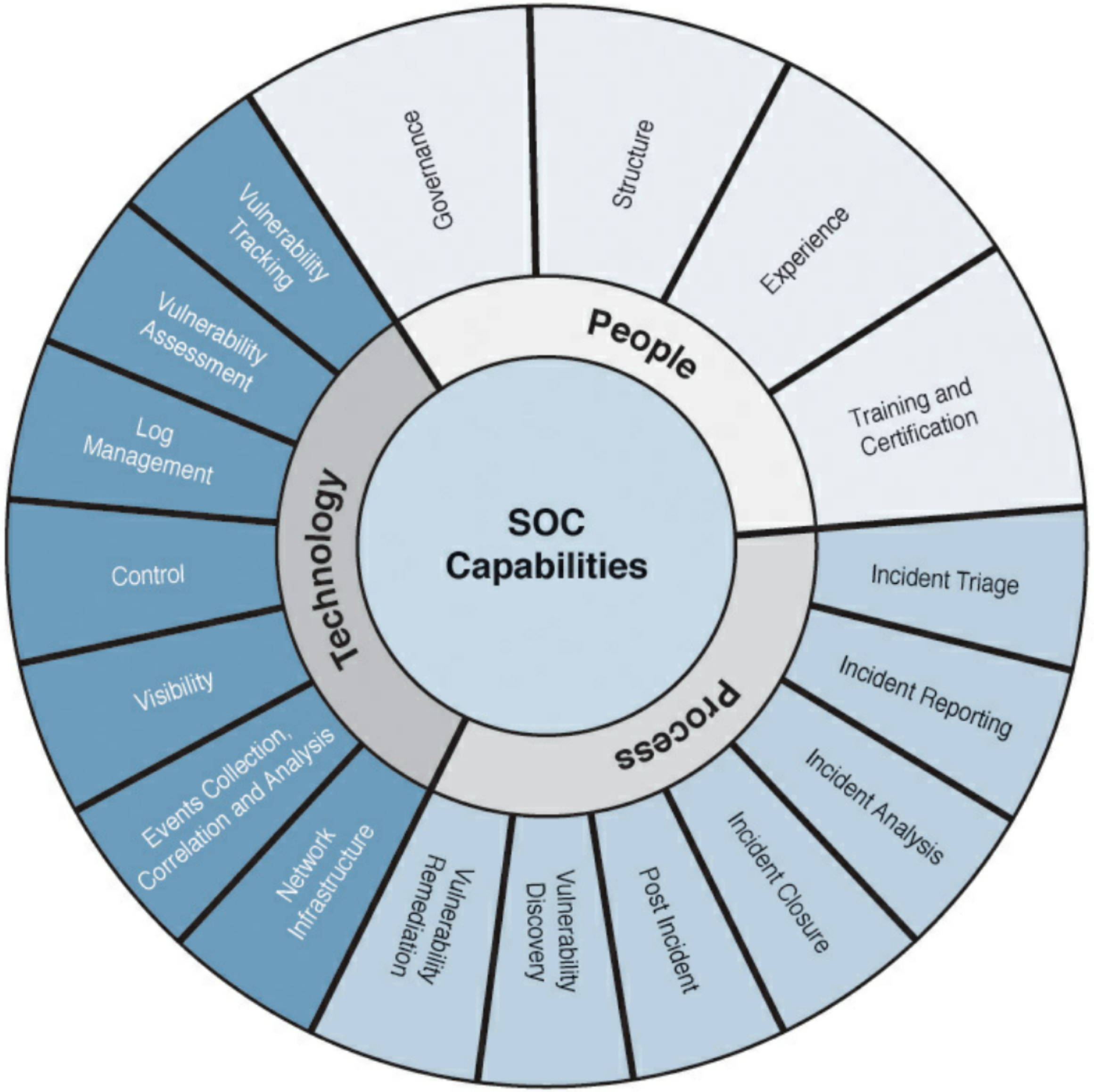
https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf



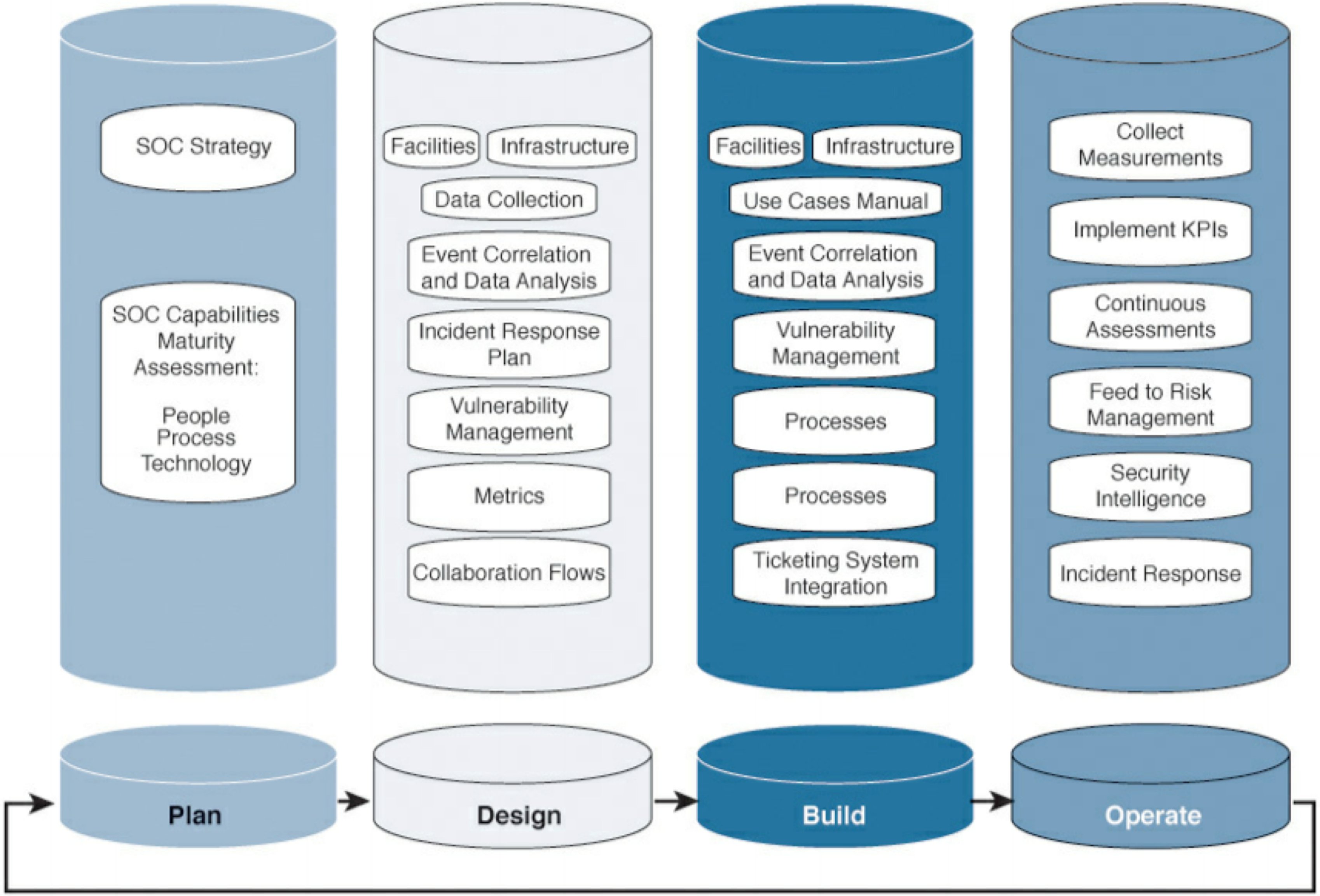
Reactive Services	***Proactive Services***	***Artifact Handling***
• Alerts and Warnings • Incident Handling • Incident analysis • Incident response on site • Incident response support • Incident response coordination • Vulnerability Handling • Vulnerability analysis • Vulnerability response • Vulnerability response coordination	• Announcements • Technology Watch • Security Audits or Assessments • Configuration and Maintenance of Security • Development of Security Tools • Intrusion Detection Services • Security-Related Information Dissemination	• Artifact analysis • Artifact response • Artifact response coordination
		Security Quality Management
		• Risk Analysis • Business Continuity and Disaster Recovery • Security Consulting • Awareness Building • Education/Training • Product Evaluation or Certification

Fig. 19 CSIRT Services list from CERT/CC

https://www.sei.cmu.edu/reports/03hb002.pdf



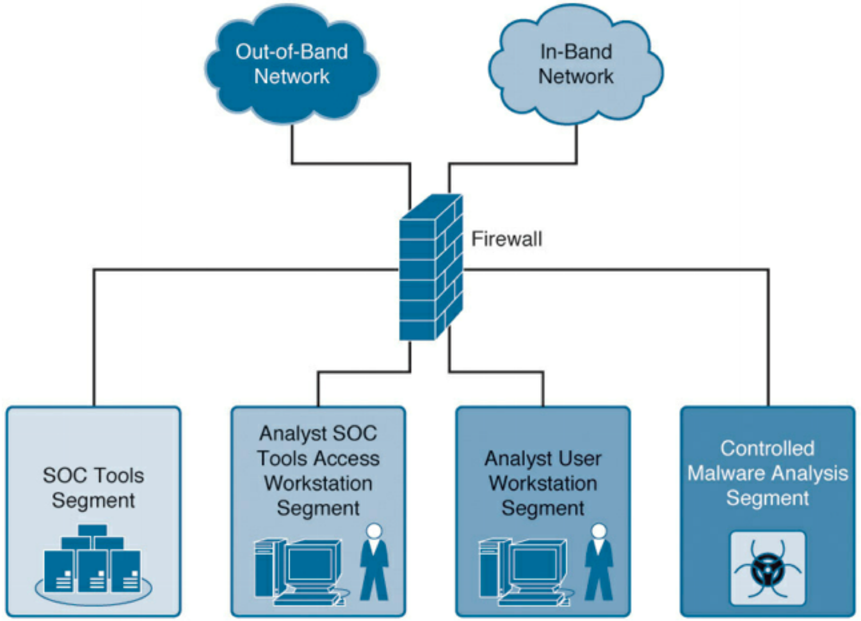
Muniz, Joseph. Security Operations Center: Building, Operating, and Maintaining your SOC



Muniz, Joseph. Security Operations Center: Building, Operating, and Maintaining your SOC

Protecting Security Operations

- Isolate SOC tools
- Operate as compromised
- Operate controlled analysis environments
- Operate controlled services



Out-of-Band Network
In-Band Network
Firewall
SOC Tools Segment
Analyst SOC Tools Access Workstation Segment
Analyst User Workstation Segment
Controlled Malware Analysis Segment

Figure 5-5 *Logical SOC Network Segmentation*

Muniz, Joseph. Security Operations Center: Building, Operating, and Maintaining your SOC

Analyst skillsets

- Analytical mindset
- Linux/Unix system administration
- IDS/IPS/Netflow
- TCP/IP and the OSI-model
- Malware reverse engineering
- Log analytics
- Vulnerability assessments
- Programming/Scripting
- OS internals and filesystems
- Communication skills

https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

Bibliography

- Muniz, Joseph. *Security Operations Center: Building, Operating, and Maintaining your SOC*
- Roberts, Scott J; Brown, Rebekah. *Intelligence-Driven Incident Response: Outwitting the Adversary*
- Liska, Allan. *Building an Intelligence-Led Security Program*
- Taylor and Francis. *Understanding the Intelligence Cycle (Studies in Intelligence)*
- Bollinger, Jeff; Enright, Brandon; Valites, Matthew. Crafting the *InfoSec Playbook: Security Monitoring and Incident Response Master Plan*, O'Reilly Media.
- Gilman, Evan. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media.
- Wheeler, Evan. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up.* Elsevier Science.
- Chuvakin, Anton; Schmidt, Kevin; Phillips, Chris. *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Elsevier Science.
- Talabis, Mark. *Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data*. Elsevier Science.
- Tan, J. 2001. Forensic readiness. *Cambridge*.
- Rowlingson, R. 2004. A ten step process for forensic readiness. *Interna- tional Journal of Digital Evidence*
- Grobler, C., Louwrens, C., & von Solms, S. H. 2010. A multi-component view of digital forensics.
- Roger, A. E. & Achille, M. M. 2012. Multi-perspective cybercrime investi- gation process modeling.
- Bejtlich, R. 2004. *The Tao of network security monitoring: beyond intrusion detection*. Pearson Education.
- Bejtlich, R. 2013. *The practice of network security monitoring: understand- ing incident detection and response*. No Starch Press.
- Brotherston, L. & Berlin, A. 2017. *Defensive Security Handbook: Best Prac- tices for Securing Infrastructure*.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.

Tools

- Suricata IDS/NSM: https://suricata-ids.org
- Bro NSM: https://www.bro.org
- Snort IDS: https://snort.org
- Cuckoo Sandbox: https://cuckoosandbox.org

- VirusTotal: https://virustotal.com
- Talos: https://www.talosintelligence.com
- URLQuery: https://urlquery.net

Resources

- https://acsc.gov.au/infosec/index.htm
- https://www.enisa.europa.eu/publications
- https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
- https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/ (Norwegian)