Building a Cyber Defense Center in a highly regulated Environment

„The bitter sweet Symphony“

Content

- What is the difference?
- What are the regulations and requirements?
- Integration into an organization
- Building and growing the team
- Processes, tools, and people
- Surviving constant audits

What is the Difference?

Failures hurt!

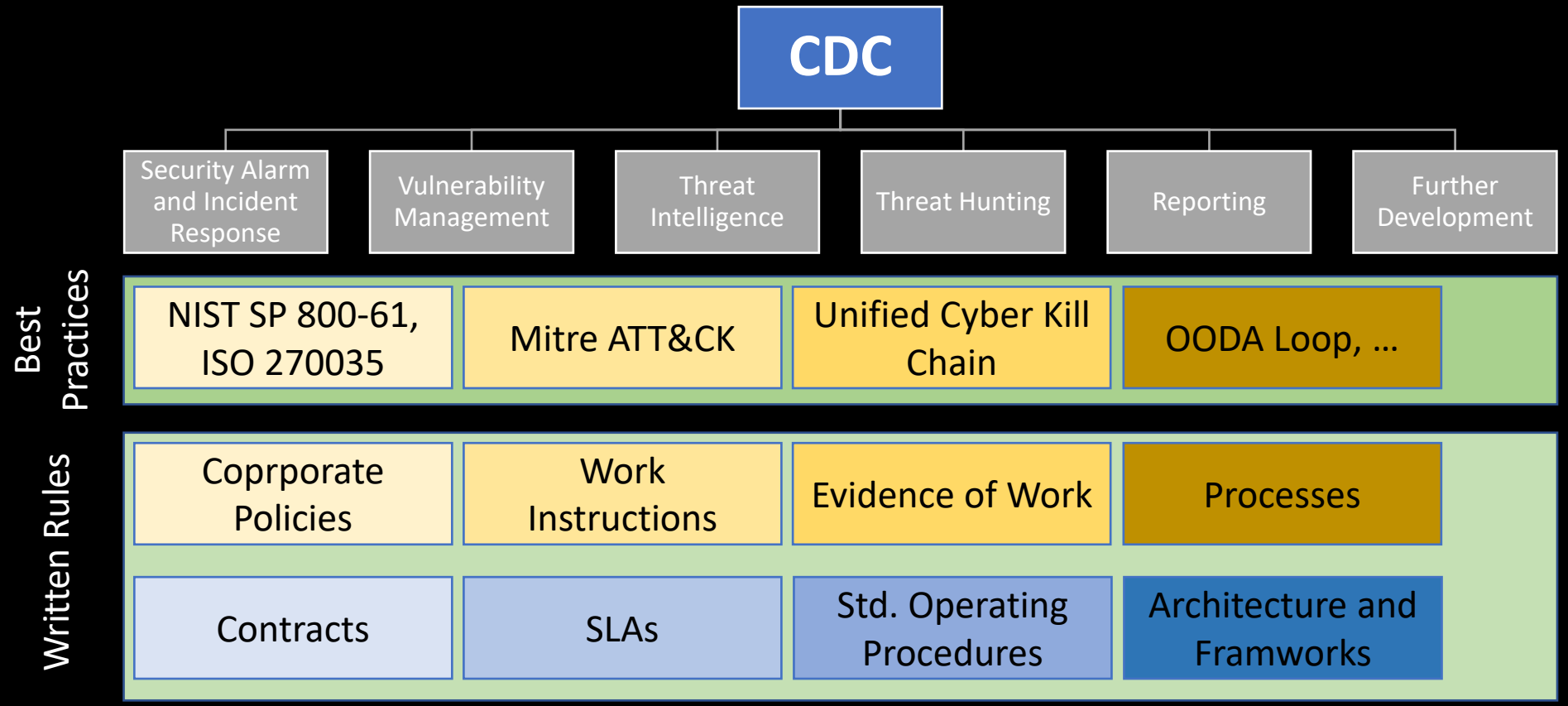
Normal CDC

CC BY 2.0

What is the difference?

Kritis CDC

Pixbay


CDC
Security Alarm and Incident Response
Vulnerability Management
Threat Intelligence
Threat Hunting
Reporting
Further Development
Best Practices
NIST SP 800-61, ISO 270035
Mitre ATT&CK
Unified Cyber Kill Chain
OODA Loop, …
Written Rules
Coprporate Policies
Work Instructions
Evidence of Work
Processes
Contracts
SLAs
Std. Operating Procedures
Architecture and Framworks

ISO 27001

- ISMS program framework
- ISO 27001 certification
- Can be easily combined with other standards, like NIST SP 800-61 instead of ISO 27035

A.8 Asset Management, incl. Information Classification

A.11 Physical and environmental security

A.12.1 Operational procedures and responsibilities

- Change Management
- Separation of development, testing, and operational environments

A.12.2 Protection from malware

A.12.4 Logging and monitoring

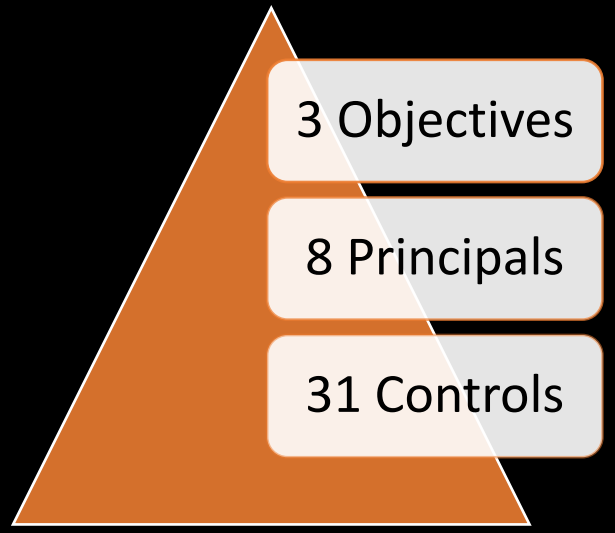
A.12.6 Technical vulnerability management

A.16 Information security incidents management!!!

PCI DSS

- As soon as you come in touch with creditcard data
- Good collection of security requirements
- Yearly audits, if you are big enough
- Watch out for new PCI DSS 4.0 requirements!

SWIFT CSCF



Secure your environment

- 1. Restrict Internet access
- 2. Segregate critical systems
- 3. Reduce attack surface & vulnerabilities
- 4. Physically secure the environment

Know and limit access

- 5. Prevent compromise of credentials
- 6. Manage identities and segregate privileges

Detect and respond

- 7. Detect anomalous activity to system or transaction records
- 8. Plan for IR & information sharing

SWIFT Customer Security Controls Framework | SWIFT - The global provider of secure financial messaging services

MaRisk, BAIT & VAIT, TIBER-DE

- Basel I to III → German Banking Act (KWG) → MaRisk → BAIT for banks and VAIT for insurance agencies
- MaRisk "Circular 09/2017 (BA)" and BAIT "Circular 10/2017 (BA)„
- High-level governance requirements, which must be fulfilled from top to bottom, and from left to right

AT 4.3.1 Organisational and operational structure	AT 4.3.2 Risk managment and risk control process	AT 4.3.3 Stress tests
AT 4.3.4 Data management, data quality and aggregation of risk data	AT 5 Policies + AT 6 Documentation	AT 7.1 Personal
AT 7.2 Technical-organizational equipment	AT 7.3 Contingency plan	...

Log retention

- PCI DSS v3.2:
  - 1 year
- BAIT 10/2017:
  - 5 years for business, control, and supervision documentation
- SWIFT CSC v2020:
  - Operator PC, database, firewall, 31 days
  - Video images, 3 months
  - Physical access logs, 12 months
  - SWIFT interface apps, 12 months
- EU-GDPR:
  - max 10 years, with justification

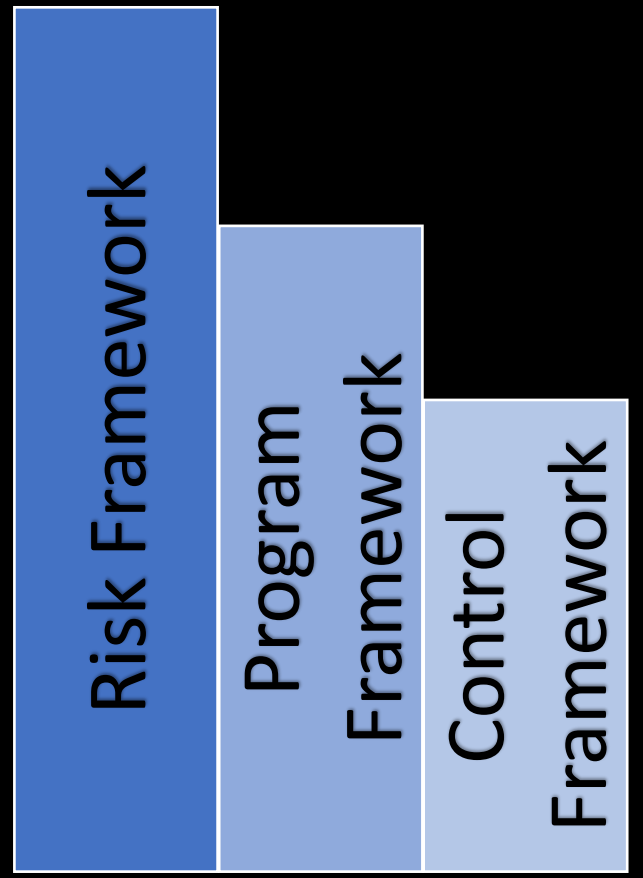
Requirement Matrix

ID#	Standard	Requirement / Topic	NIST CSF Function					BSI IT-Grundschutz	DSGVO	PCI-DSS v3.2
			IDENTIFY (ID)	PROTECT (PR)	DETECT (DE)	RESPOND (RS)	RECOVER (RC)			
1	ISO 27001	Scope	X					BSI-Standard 200-2, Kapitel 1 Einleitung		
2	ISO 27001	Normative references						BSI-Standard 200-1, Kapitel 11.1 Literaturverzeichnis		
3	ISO 27001	Terms and definitions						BSI-Glossar der Cyber-Sicherheit, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.htm		
4	ISO 27001	**Context of the organization**								
4.1	ISO 27001	Understanding the organization and its context						BSI-Standard 200-2, Kapitel 3.2.1 Ermittlung von Rahmenbedingungen ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie		
4.2	ISO 27001	Understanding the needs and expectations of interested parties						BSI-Standard 200-2, Kapitel 3.2 Konzeption und Planung des Sicherheitsprozesses		
4.3	ISO 27001	Determining the scope of the information security management system						BSI-Standard 200-2, Kapitel 3.3.4 Festlegung des Geltungsbereichs und Kapitel 8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung		
4.4	ISO 27001	Information security management system						BSI-Standard 200-1, Kapitel 3 ISMS-Definition und Prozessbeschreibung BSI-Standard 200-2, Kapitel 2 Informationssicherheitsmanagement mit IT-Grundschutz ISMS.1 Sicherheitsmanagement		

The Organization

Making things fit.

Governance Structure



Integration into an Organization

- Goals and clear responsibilities
  - **Tasks**: detect, respond, develop, CTI, active defense, hunting, ...
  - **Scope**: internal, customer service, phishing, malware, APT, server, clients, CDC hierarchy
  - **Interfaces**: inter-corporate, customers, external (open, closed)
  - **KPI**s and **SLA**s
- Repeated communication helps the people
- **Cultural differences**: crit. infra. companies tend to be bureaucratic and traditional - cybersecurity engineers are creative people looking for a solution + behavioral patterns and office politics are a hurdle for many engineers
- CDC **horizontal**: CISO vs CIO → very good relationsship is crucial
- CDC **vertical**: directly reporting to C-level, or security-minded senior manager inbetween
- **Adapt** existing processes, models and terms
- **Reframe the fears** and concerns the works-council often has
- Develop and train Incident Response together with affected departments, let every department have a „CDC delegate“ or CERT member, that take care of updating IR-plans, make them part of your virtual CDC team → **relationship is crucial** vs. cultural issues
- **Make cybersecurity everybodys job!**

The CDC

Build to adapt.

From Security Event to Incident Response

- Which use-cases? Sources:
  - **IT Risk Management**, mitigational meassure
  - **ISMS**, protection level, higher level → more monitoring
  - **TTP**: Mitre ATT&CK groups with financial intent → lookup their TTPs → develop use-cases to detect them
  - **CTI**: constant monitoring of the threat landscape to adapt fast
- Log sources
  - input-driven, output-driven, hybrid
  - Your budget is the limit.
  - Change management, testing, keep alive, monitoring, separation of duties
- What use-case first? Priorities for...
  - Development
  - SIEM → Analysis → Incident Response

Setting SIEM Use-Case Criticality

#	Unified Kill Chain	Cyber Kill Chain®	Laliberte	Nachreiner	Bryant	Malone	MITRE ATT&CK	UKC after literature	UKC after Red Team	UKC after Red Team	UKC after Red Team	UKC after Red Team
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9
10	Discovery					14	10	10	11	11	11	10
11	Privilege Escalation					17	14	14	10	10	10	11
12	Execution					18	12	12	14	14	14	12
13	Credential Access						15	13	12	12	12	13
14	Lateral Movement						16	17	13	13	13	14
15	Collection						8	15	17	17	17	17
16	Exfiltration							16	15	15	15	15
17	Target Manipulation								16	16	16	16
18	Objectives											

The Unified Kill Chain

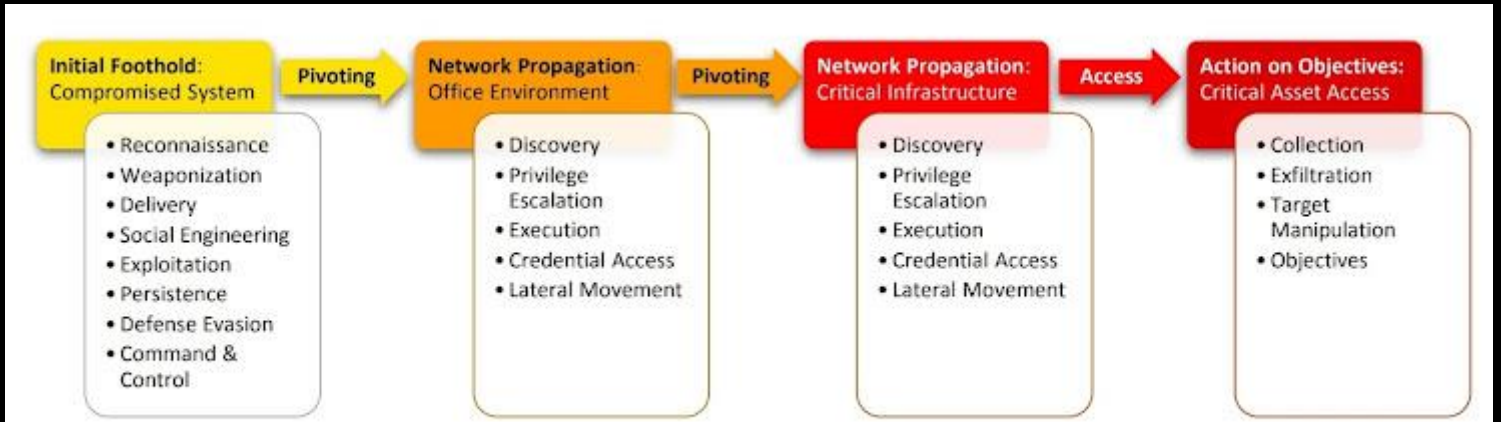
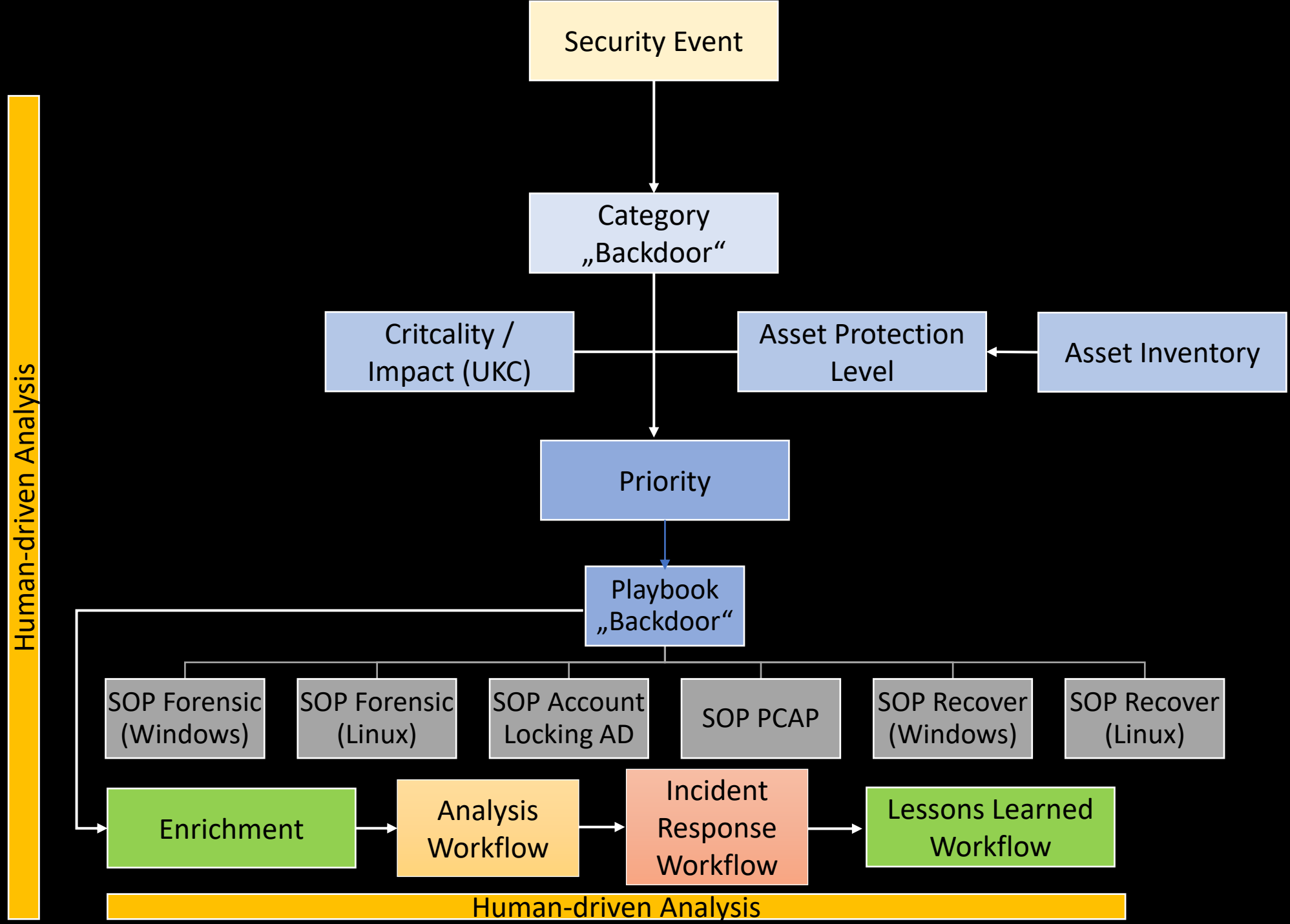


Figure 1 – An attack path abstraction for a segmented network based on the Unified Kill Chain

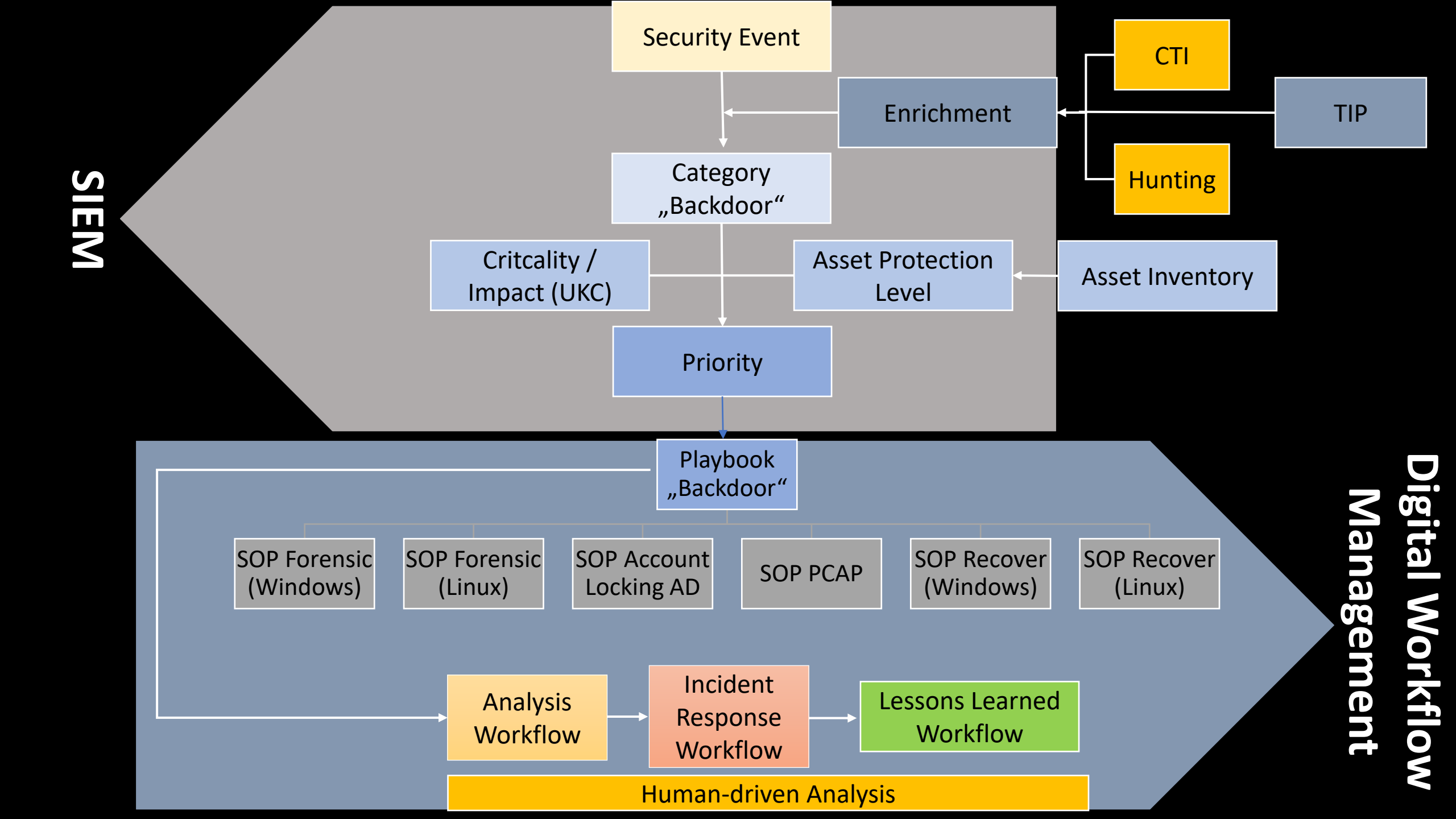
Example

UKC phase	Criticality of potential incident	Priority of triage based on asset
Initial Foothold • Reconnaissance • Weaponization • Delivery • Social Engineering	Low	Low
Initial Foothold • Exploitation • Persistence • Defense Evasion • Command & Control	Medium	High
Network Propagation (Office Network)	High	High
Network Propagation (internal/high protection-level Network	Critical	Critical
Action on Objectives (on "Crown Jewels")	Crisis	Crisis


Security Event
Category „Backdoor“
Critcality / Impact (UKC)
Asset Protection Level
Asset Inventory
Priority
Playbook „Backdoor“
SOP Forensic (Windows)
SOP Forensic (Linux)
SOP Account Locking AD
SOP PCAP
SOP Recover (Windows)
SOP Recover (Linux)
Enrichment
Analysis Workflow
Incident Response Workflow
Lessons Learned Workflow
Human-driven Analysis
Human-driven Analysis

Fully automated Workflow(s)

- More automation = less + central documentation
- More automation = less time
- More automation = less failures
- More automation = less media disruption
- More automation = easier hand-overs (shift duty)
- More automation = easier integration of customers


SIEM
Security Event
CTI
Enrichment
TIP
Hunting
Category
„Backdoor“
Critcality /
Impact (UKC)
Asset Protection
Level
Asset Inventory
Priority
Digital Workflow
Management
Playbook
„Backdoor“
SOP Forensic
(Windows)
SOP Forensic
(Linux)
SOP Account
Locking AD
SOP PCAP
SOP Recover
(Windows)
SOP Recover
(Linux)
Analysis
Workflow
Incident
Response
Workflow
Lessons Learned
Workflow
Human-driven Analysis

Managed Security Service Provider

- Only sell standard solutions or die!
- Bring the customer to your world, use standardized interfaces, processes, use-cases, playbooks
- Catalogue: SIEM use-cases. Log sources
- Fulfill regulartory requirements of the customer
- Customer must have baseline security standard
- CERT team at customer site
- Access to customer machines? Active defense?
- 24/7 if customers wants it, he also has to provide a 24/7 SPOC which can act and give answers to analysts
- Contract, SLA → just standard
- Regular customer service / onboarding calls help at the beginning but are expensive later (due to misuse)

You can just sell, what you can deliver TODAY.

Specials

- Have physical access control for your CDC offices and data centers
- Build a lab, disconnected from the rest of IT
- Have a dedicated Internet connection, not directly bound to your company to bring the lab and other research equipment online
- Make your CDC an “IT island”, don’t connect to the central Active Directory, have external telephone conference providers, have internal collaboration tools, and so on
- Convince the BCM folks that it is crucial to bring the SIEM and CDC back up and running very early

The Team(s)

The only thing that makes a differnce.

Team Structure

- Fit the goals and don‘t overload people with tasks
- Clear responsibilities
    - IT operation, tools and lab
    - Analysts / Tickets / Hotline / 24x7 (Playbooks, SOPs)
    - Senior analysts to verify what is left
    - Cyber Threat Intelligence (CTI)
    - Threat Hunter
- The last three roles can overlap
- CDC manager: A people gal/guy, technically top-notch, great communicator.
- Shift duty manager: senior security engineer
- Challenge: Find the ballance between separation of duties and effective information exchange. Always foster an open-minded and forward-thinking team.

Unclear CDC Roles

- Firewall, AV, EDR, mail gateway administration
- Vulnerability manager
- CERT, Incident Response, Forensics
- Business development
- Customer service

Building and growing the Team 1/2

- Always encourage your team to take responsibility.
- Teach them to think forward and take action!
- Don‘t put your people in boxes, let them evolve freely, cybersecurity people are creative people
- Try to reach and keep at least 60% of senior security engineers
- Diversity is good to break up old ways of thinking and structures but can also lead to conflicts between team members.

Take care of people with a negative / destructive attitude!

Building and growing the Team 2/2

- Let young security analysts do hunting and take responsibility during hot IR phases, this helps asking the right questions and to understand an attacker (riding a bike cannot be learned from watching youtube), give them senior support but not too early
- Let different kind of people work together on a tasks, so they form a small team, rotate the people to create a strong team-spirit

Transfer „bad apples“ and low performers

→

The job market is full of good people that like to change!

Taking over an existing Team

- Try to give everyone the role and responsibility that fits her/his strength
- For a **limited period only**: Help low performers to become better (tiny steps) if they keep failing, find a better place for them.
- Majority is young and unexperienced, give them development goals, show them a path for their career, and give them top-notch trainings
- Much more experienced team-members (employes close to retirement) can support technically and with the organizational hurdles to make the work-life of the younger engineers more efficient.

During the build-up Phase: When to protect the Team and when not

- **Protect**:
  - External inqueries, customers, other departments and so on
  - Team mates* that tend to overestimate their power and possibilities
  - Team mates* that cannot say „No.“
  - Working regularly in a shift model, or during night. Better try to give this job to external people or people that already do monitoring / help-desk service during the night.
- **Don‘t protect**:
  - Team mates* that want to make experiences and take responsibilities, encourage them!
  - Low performers & procrastination
  - Failures!
  - Team mates* that do their job somehow but are unwilling to learn
  - Team mates* with toxic attitude and everyone else with a visible Hybris and an underdeveloped ability to reflect her-/hisself

Empowerment, trust, and respect will create a bombastic Team!

… MAYBE!

* Includes the CDC manager(s)

„Threat Actor“ →

Speak the same Language

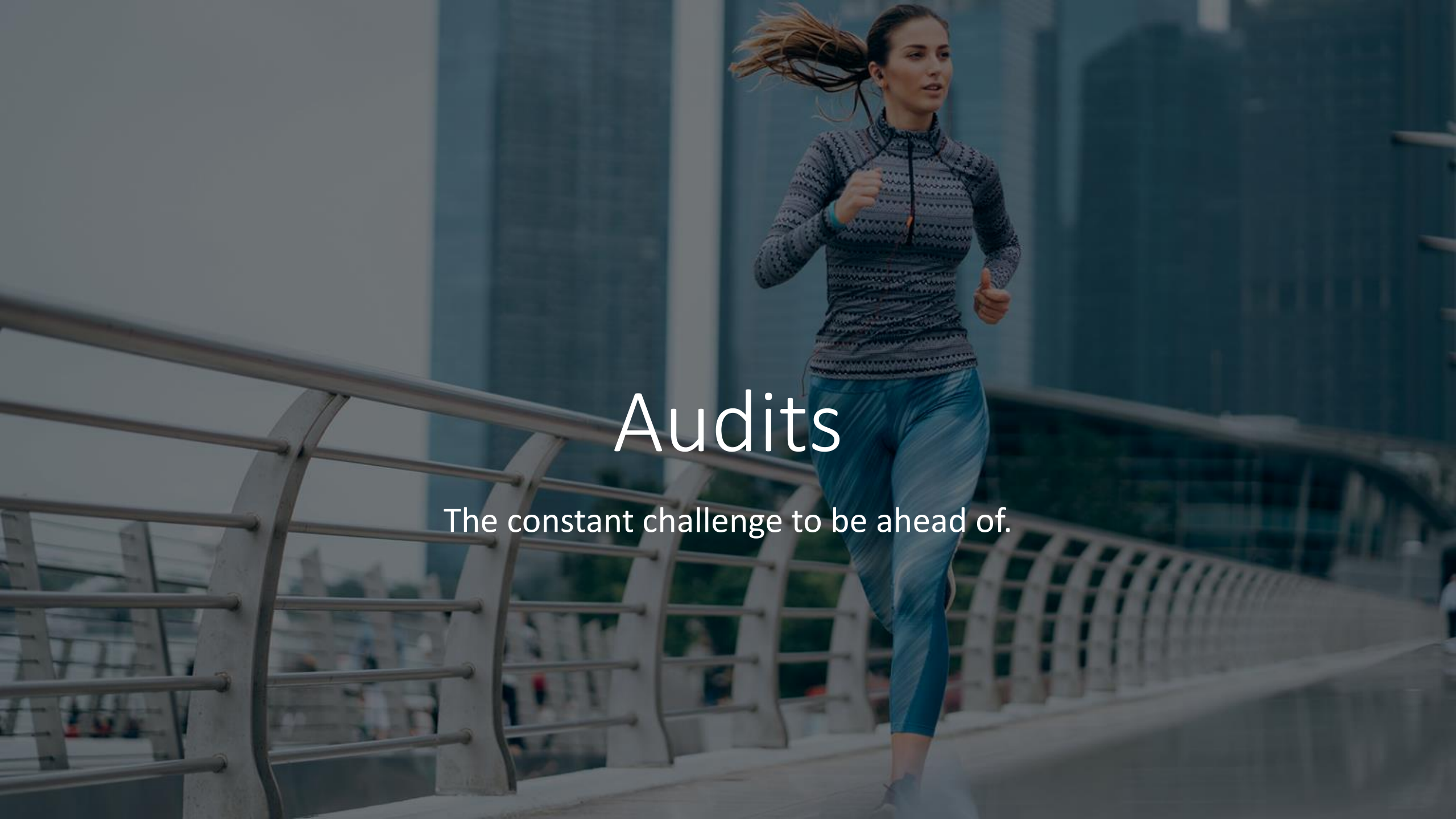
- Avoid ambiguities, foster the behavior of asking questions to gain clarity
- Standards, like ISO 27035 or NIST SP 800-61
- Models, methodology, and terms
    - Playbook, SOP
    - Diamond model → to ask the right questions, create adversary persons
    - Lockheed Martin „Kill Chain“ → for management
    - Paul Pols‘ „Unified Kill Chain“ → prioritisation of use-cases, for the analysts, for CERT
    - Mitre ATT&CK, TTPs → use-cases, CERT
    - 5 Ds: Deter, Detect, Deny, Delay, and Defend → CERT
    - OODA loop → CERT, response + deception + denial
    - Threat actor, campaign, group, intrusion set … → avoid terms that cause biases

Consultants and Service Providers

- Status quo: There are only a few really good people out there, and they are already booked by high-profile clients
- **Does**
  - Build up or maintain IT systems / products
  - Standard operational tasks
- **Don‘ts**
  - Expect them to be creative
  - Expect them to know what they should do (*psst* often they have never done the tasks before!)
  - Make things fit into a bigger picture (they often lack business context)

Remember, the good people are already bound to other clients.

Senior consultants become managers, junior consultants do the operational part.



Audits

The constant challenge to be ahead of.

Surviving constant Audits – Common Pitfalls

- Changes happen without documentation, review, or without approval
- Assume you can just do it along with your normal work, plan capacity
- You cannot explain why you monitor a specific log source or why you have a SIEM use-case for attack A but not for B.
- Processes are undocumented
- Process outcome is undocumented
- Incident investigation documents can be changed/deleted w/o changelog or approval
- Missing fallback and BCM planning
- No separation of duties, between use-case writing, testing, approval, and usage

Surviving constant Audits – Preparation

- Have uptodate governing rules, like
  - Policies
  - Standard Operating Procedures
  - Playbooks
- Only write down in your policy what you can fullfil in real-life!
  - You need a policy / SOP for everything you do! And you have to review it once a year at least! With a review process and an approval process!
- Have all documentation of your work in a central place, ready to be handed over to auditors at any time.
- Have small & simple diagrams to explain what you do.
- Let others review it!
- Ask the auditors to review updates.
- Have a small team that takes care of every audit.
- Create a good atmosphere and relationship between the auditors and your team.

Plan Do Check Act

Plan	Do	Check	Act

• Clear requirements
• Clear responsibilities
	• Policies, playbooks, SOPs
	• People, processes, tools
		• Lessons learned for
		  • incident, failures
		  • things work great – copy it! communicate it!
			• Improvements within the CDC
			• Improvements within the organisation
			• Maturity Model (SOC CMM)

Feedback and Questions?

Always feel free to contact me.

Contact

Thomas Biege

Cyberdefense-consulting@protonmail.com and you can find me on LinkedIn