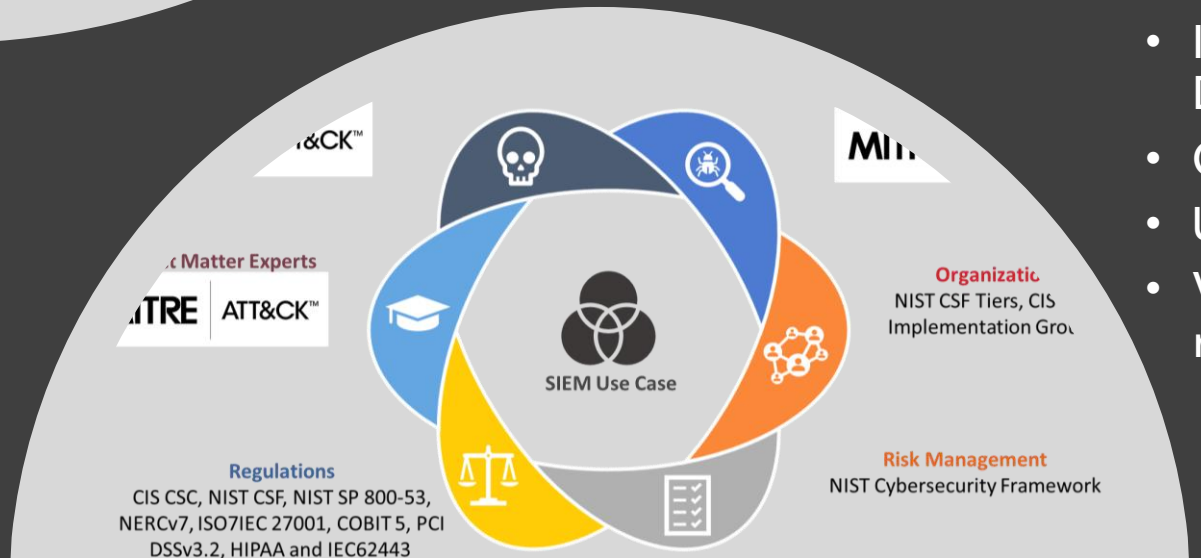
Lucerne University of Applied Sciences and Arts

Master of Advanced Studies in Information Security

Methodology to select Security Information and Event Management (SIEM) Use Cases

Speaker Introduction: Pascal Imthurn

- Head Cyber Defense Services
- 20 years of experience in IT Sec
- Milestones:
  - ISPIN: Developed & managed Cyber Defense Services
  - Open Systems: Security Architect
  - UBS: Global Head of SOC
  - Various: Linux firewall developer, reverse engineer, threat analyst



Public Link: www.siemucsm.com

Introduction - Motivation

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 10

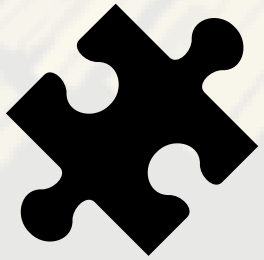
The primary objective of this research is to mitigate the impact of cyberattacks by providing a method to best match the current attack methodologies with detection capabilities.

[] Image source of title page: https://datavizproject.com/data-type/sunburst-diagram/

Introduction – Problem Statement

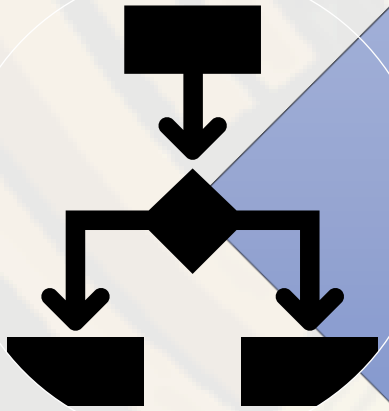
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 9

This study proposes to investigate a possible methodology in assisting organisations and cybersecurity professionals in selecting SIEM Use Cases based on the catalogued techniques in the Mitre Att@ck Framework. This methodology should consider the respective technical and organisational environment, internal and external requirements, as well as best practices and the available security know-how of the company or organisation.



Introduction – Research questions

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 10



If cybersecurity risks are managed by frameworks and standards, can we combine the requirements listed in these documents with actual threat data to drive the SIEM Use Case selection process?

Main

- Use Case Selection
- Threats & Detection
- Standards
- Selection

Sub

Literature Review – Academic research

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 20

Following types of research paper have been identified:

The focus lies with the SIEM technology only

The focus is on specific detection capabilities

- The lack of research papers in the area of SIEM technologies can be an indicator that the area of SIEM technology is primarily driven by vendors
- There are however many research papers on various detection technologies. The research is mostly focused on a single topic
- There is no general SIEM Use Case design approach. It is generally assumed that organisations know how to protect their assets.

The answers to protect the identified risks are too vague and lead to alternative ways of interpretation and implementation

Literature Review – Threat resources

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 21

Sources reviewed:

- Manual research
- Vendor Reports
- Disclosed Vulnerabilities
- **Mitre Att&ck Framework**
- Hackmageddon
- Exploit-DB

Inaccurate and labor-intensive

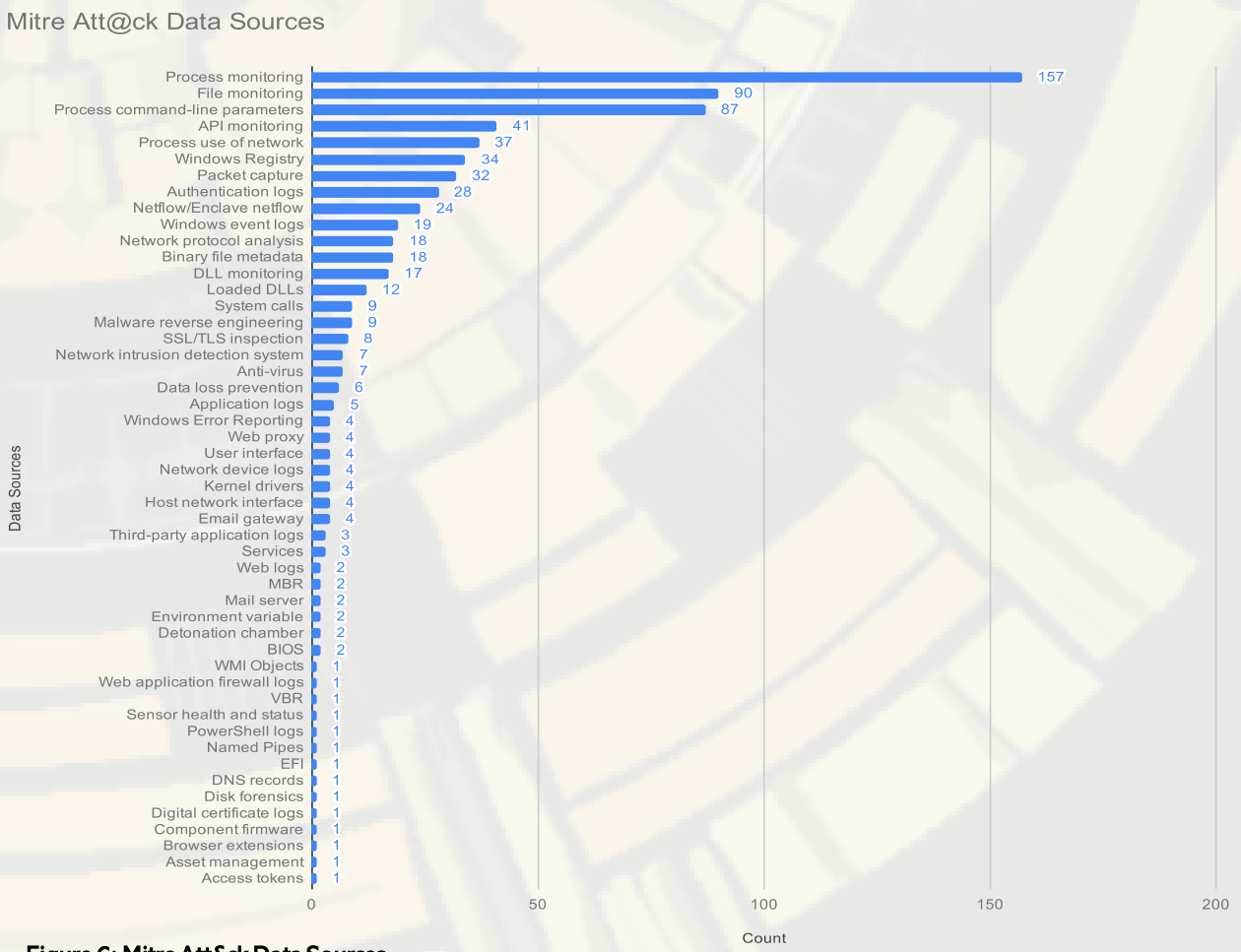


Figure 6: Mitre Att&ck Data Sources

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 32

Literature Review – Vendors

Vendors reviewed:

- Exabeam
- Logpoint
- RSA
- AlienVault
- Splunk
- Exploit-DB

Everyone measures differently

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 43

Approaches	Count
Compliance	2
Insider Threats	1
Advanced Security	2
Best Practise	1
Custom	2

Table 1: Approaches recommended by the analysed vendors
Source: *Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 32*

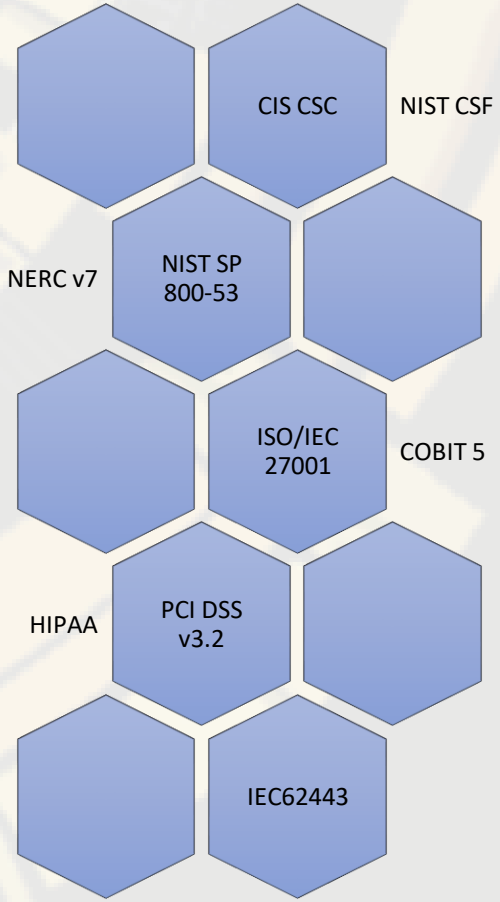
1. SIEM Use Cases are selected by compliance
2. The data shows that the best practices of the respective vendors are used for marketing purposes
3. Customer SIEM Use Case library based on identified risks or motivators.

Literature Review – Cybersecurity Standards & Frameworks

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 48

Identified Mappings:

- NIST CSF Core
- CIS Controls v7.1 Mapping for Implementation Groups
- AuditScripts
- AuditScripts CSC Manual Assessment Tool
- CIS Controls v7.1 Mapping to NIST CSF



5 mapping files for further research

Literature Review

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 49

No holistic approach to solving the detection problem. Researchers are focused on solving or improving methods in advancing the capabilities of unique technology.

Manual research to acquire current threats is not recommended as an individual. The amount of time invested, the lack of a unified taxonomy on how to record findings.

Fragmented and marketing driven. Save bet implementations are compliance driven.

Readily available mapping files. Support organisations who comply with existing frameworks

Rely on large public dataset

Literature Review – Conceptual Framework

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 49

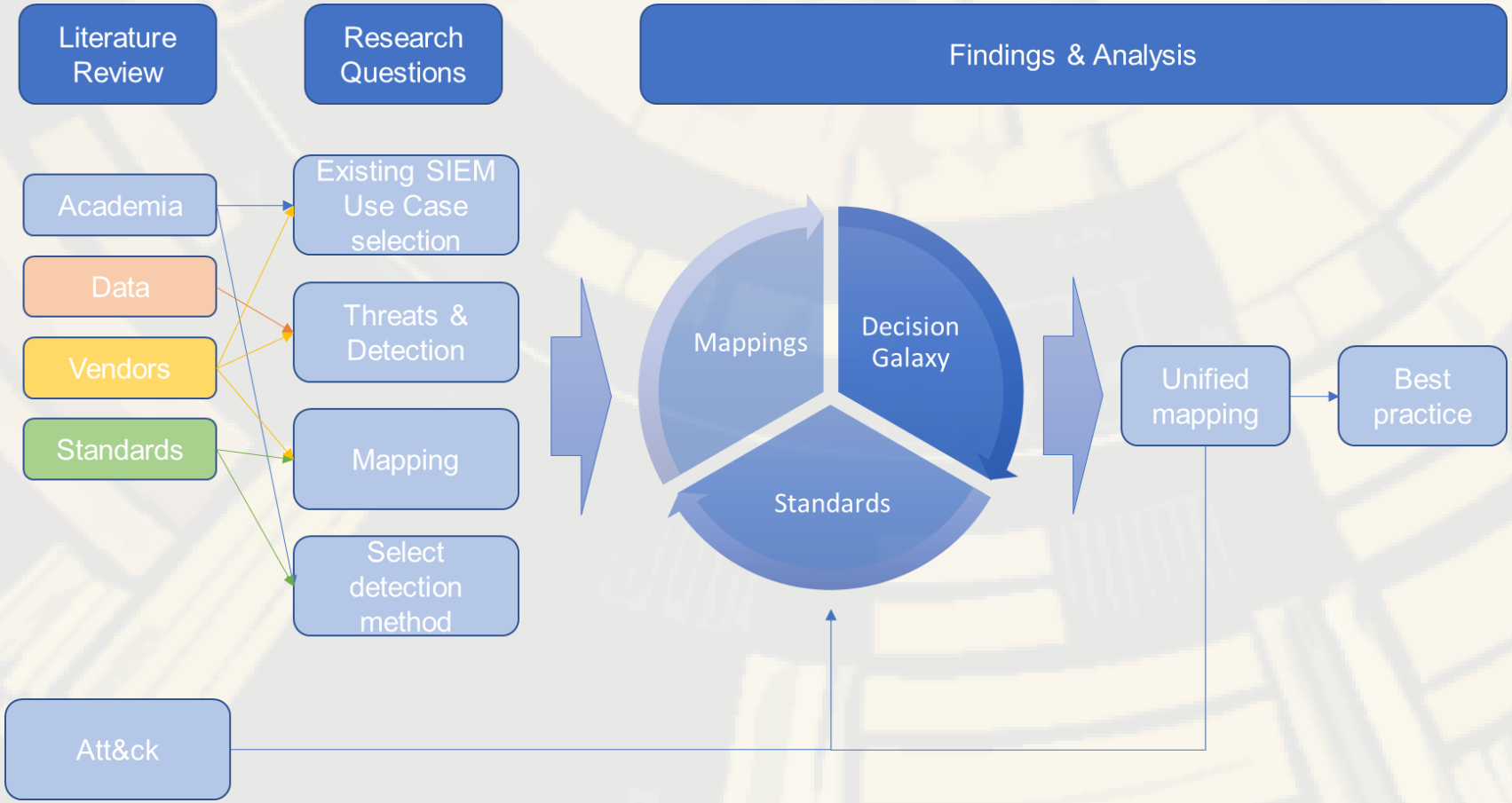


Figure 2: Conceptual framework of the thesis

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 49

Design & Methodology – Limitations

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 58

No external influence	SIEM "Use Case"	Att&ck Framework Detection = SIEM Use Case	Detection capability = Use Case
Not measuring effectiveness of SIEM	Data quality of used data	NIST CSF Framework	ML is a Use Case
Application not public	Sample rate of academic writing	Data Privacy	Implementation Cost

Design & Methodology – Use Case Selection

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 60

Identify Focus Areas: (1) Van de Moosdijk and Wagenaar, (2) Perniola and Grey and (3) Faircloth

	(1)	(2)	(3)	Combination
Organisation Requirements	X	X	X	Organisation
Operational Requirements	X		X	
Compliance				Regulations
Log Management	X			Detection Capabilities
Correlation	X			
Alerting	X		X	
Response	X			
Risk Management		X	X	Risk Management
Subject Matter Experts		X	X	SMEs
Threats			X	Threats

Table 2: Combined focus area

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 60

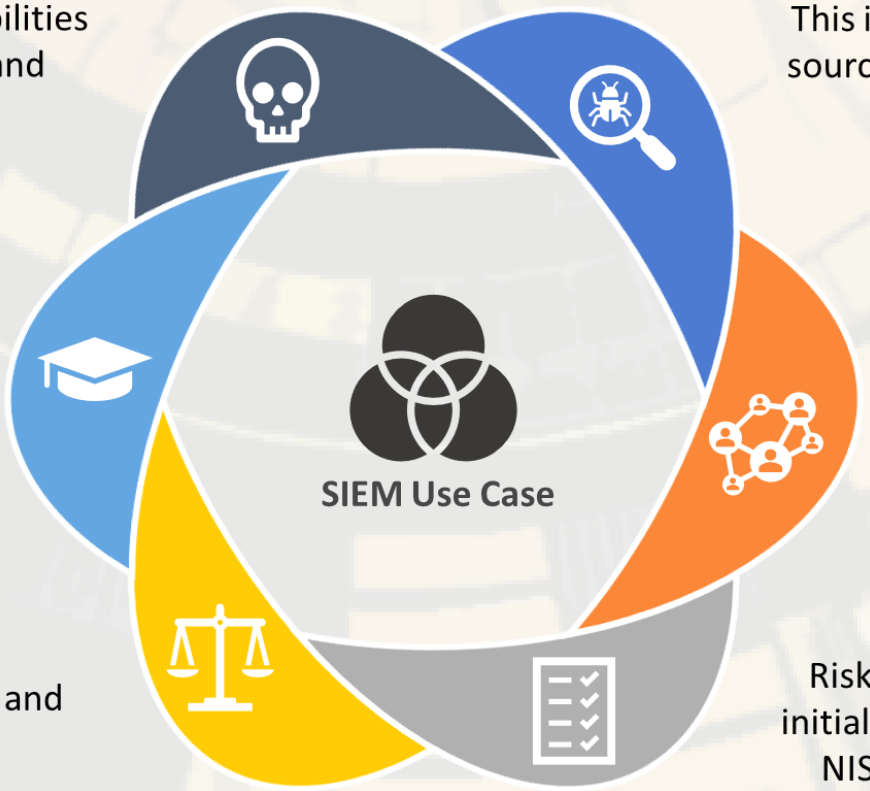
Design & Methodology – Use Case Selection "Decision Galaxy"

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 61

Threats
Actual threats such as vulnerabilities and exploits, best practises and sector goals

Detection Capabilities
This includes everything from log sources, aggregation, correlation, alerting and response

Subject Matter Experts
Experts of their respected fields of expertise such as network, operating systems, security and others



Organization
Organization and business requirements, organizational maturity and prioritization

Regulations
Regulations, standards and compliance

Risk Management
Risk Management framework, as initially stated, this work is using the NIST Cybersecurity Framework

Figure 14: Use Case decision galaxy
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 61

Design & Methodology – Use Case Selection "Simplification"

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 72

The focus areas of the SIEM Use Case selection process cover a vast expanse on influencing parameters. The Decision Galaxy can be further simplified by substitution.

Optimisation
- Organising Requirements
- Costs
- Size/Manageability

Focus area	Simplification source
Organisation (4.2.3)	NIST CSF Tiers, CIS CSC Implementation Groups
Regulation (4.2.4)	CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443
Detection (4.2.5)	Mitre Att&ck Framework
Risk Management (4.2.6)	NIST CSF
Subject Matter Experts (4.2.7)	Mitre Att&ck Framework
Threats (4.2.8)	Mitre Att&ck Framework

Table 2: Focus areas and their simplified sources
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 72

Design & Methodology – Use Case Selection "Decision Galaxy"

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 61

Threats

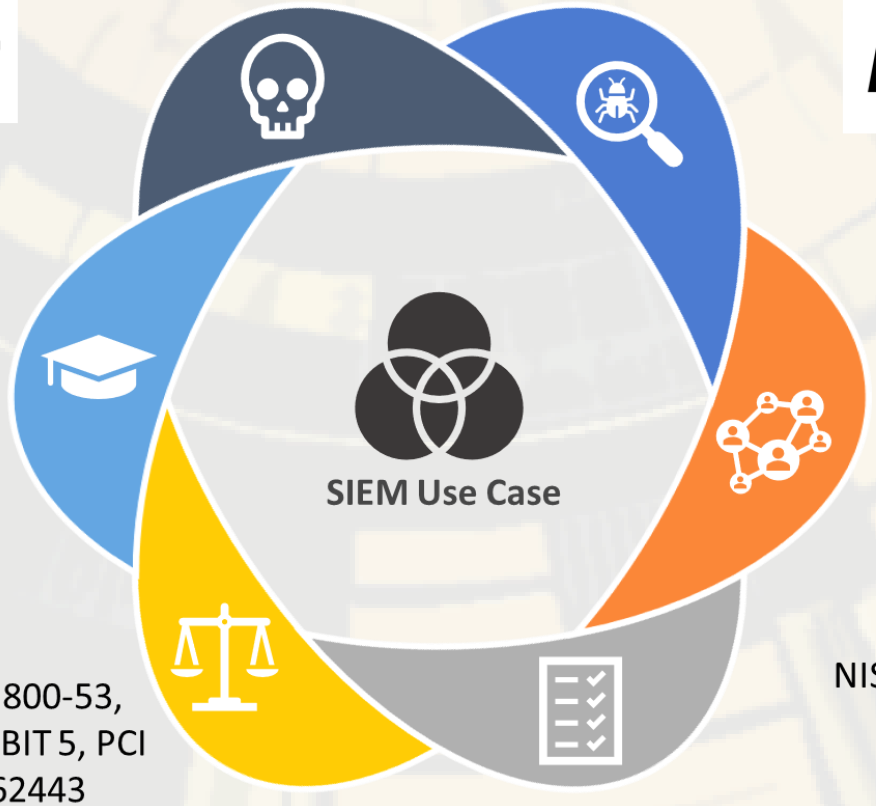
MITRE ATT&CK™

Detection Capabilities

MITRE ATT&CK™

Subject Matter Experts

MITRE ATT&CK™



Organization

NIST CSF Tiers, CIS CSC Implementation Groups

Risk Management

NIST Cybersecurity Framework

Regulations

CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443

Figure 14: Use Case decision galaxy

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 61

Design & Methodology – Threat Detection

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 72

The research in chapters 2.2.2 has shown that the Mitre Att&ck Framework has proven to be the most effective dataset available.

- Much steeper maturity increase
- More likely to be able to identify an attacker
- Distinctive gap between the Mitre Att&ck Framework and the business side of organisations.

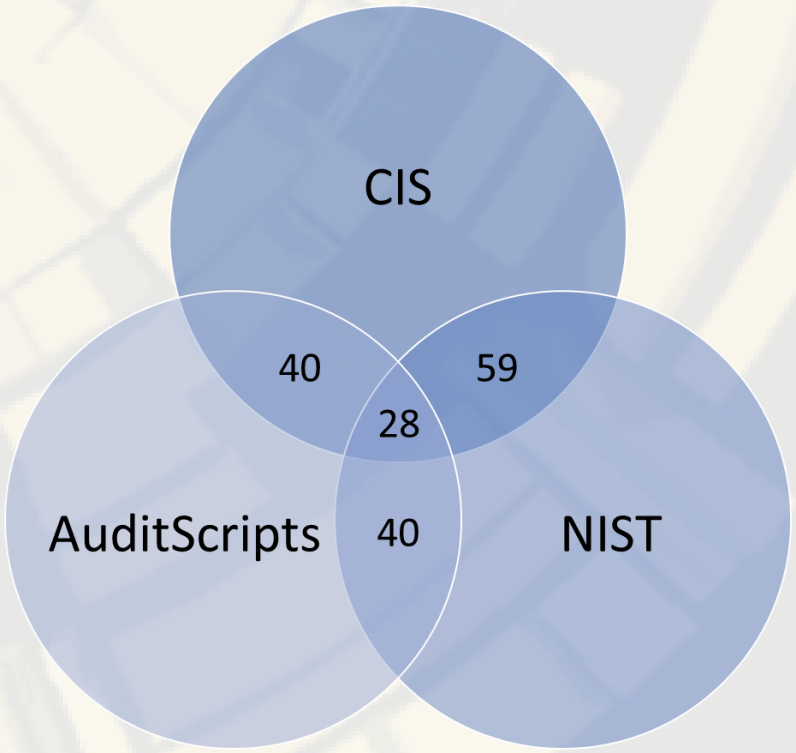
Include the decision makers

Design & Methodology – Standards Mappings

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 77

Count of Framework	Column Labels																				
Row Labels	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Grand Total
DE.AE-1	1			1		1			1			2	1		2	1					10
DE.AE-2			1			2							1		1				1		6
DE.AE-3	1		1	1	1	3	2	2			1	1	1	1	1	1					17
DE.AE-4				1		1													1		3
DE.AE-5						2			1										1		4
DE.CM-1	1						2	2				2	1		2	1			1		12
DE.CM-2																			1		1
DE.CM-3					1		1							1		2			1		6
DE.CM-4				1			2	3				1							1		8
DE.CM-5							1	2											1		4
DE.CM-6																			1		1
DE.CM-7	2	2	1	1	1		1		1			2	1		2	1			1		16
DE.CM-7													1								1
DE.CM-8			2	1	1				1		1									1	7
DE.DP-1						1													2		3
DE.DP-2						1															1
DE.DP-3						1															1
DE.DP-4						1													2		3
DE.DP-5						1															1
ID.AM-1	3	1																			4
ID.AM-2		3																			3
ID.AM-3	1										1	1			1						4

Figure 2: Comparison of mappings to NIST sub-categories
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 77



All figures shown are the count of matching CSF controls per CIS control.

Figure 21: Data comparison of CIS - AuditScripts - NIST mappings to CSC
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 79

Design & Methodology – Standards Mappings

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 77

- CIS and NIST have the most overlap
- AuditScript mapping seems to be congruent to the other two mappings

Results do not allow for a decisive decision in selecting a mapping file. It rather became apparent, that an organization can select their preferable mapping file.

The organisation simply declares which mapping file has been used.

Any of the mapping files can be used

Design & Methodology – Combined Selection Process

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 86

Att&ck and CIS mapping

Attack		CIS Subcontrol																
Process monitoring	Detection	8.3	6.2	6.3	2.8	2.9	6.7											
File monitoring		14.9	5.5	5.3	6.3	6.7	4.8											
Process command-line paramete		8.8	2.9	14.9	6.3	6.7												
API monitoring		8.8	14.9	6.3	5.3	5.4	6.7	11.3	8.3	2.8	5.5	2.9	16.6	6.2				
Process use of network		2.1	2.3	2.4	2.8	2.9	7.4	3.1	3.2	5.5	7.2	8.3	8.7	11.3	12.2	13.3	13.5	6.7
Windows Registry		5.5	6.3	6.7														
Packet capture		12.5																
Authentication logs		4.8	16.12	4.9	11.5	12.11	16.10	16.3	20.8	6.7								
Netflow/Enclave netflow		12.5	12.8	11.2	12.2	12.11	13.5	18.10	6.7									
Windows event logs		16.6	6.2	6.3	6.7													
Network protocol analysis		12.6	15.3	12.4	15.2	15.8	6.7											
Binary file metadata		7.10	6.3															
DLL monitoring		2.8	6.3	6.7														
Loaded DLLs		2.8	6.3	6.7														
System calls		2.8	8.3	13.3	14.9	6.3	5.3	6.7										
Malware reverse engineering		7.10	18.7															
SSL/TLS inspection		12.10																
Network intrusion detection syste		12.6	15.3	9.3	9.4	12.2	12.7	6.7										
Anti-virus		8.1	8.2	8.4	8.6	6.7												
Data loss prevention		13.3	13.5	14.7	14.8	14.5	13.7											
Application logs		9.5	6.3	6.7														
Windows Error Reporting		6.3	6.7															
Web proxy		12.9	12.10	7.4	7.6	7.5	13.4	6.7										
User interface		13.3	6.2	6.3	6.7													
Network device logs		9.1	9.3	11.3	13.3	15.1	15.2	15.3	6.7									
Kernel drivers		5.5	6.3	6.7														
Host network interface		9.1	9.3	11.3	13.3	15.2	15.3	6.7										
Email gateway		7.8	7.10	6.7														
Third-party application logs		3.5	9.5	3.1	3.2	6.3	6.7											
Services		6.3	5.3	6.7														
Web logs		12.9	12.10	18.10	6.7													
MBR		6.3	6.7															
Mail server		20.4	6.7															
Environment variable		8.8	6.3	6.7														
Detonation chamber		7.10	18.7	6.7														
BIOS		8.3	5.3	5.4	6.7													
WMI Objects		6.3	6.7															
Web application firewall logs		18.10	12.9	6.7														
VBR		6.3	5.3	5.4	6.7													
Sensor health and status		6.2	6.3	6.7														
PowerShell logs		8.8	2.9	14.9	6.7													
Named Pipes		6.3	6.7															
EFI		6.3	5.3	5.4	6.7													
DNS records		7.7	8.7	6.7														
Disk forensics		14.9	6.3	5.3														
Digital certificate logs		1.8	6.7															
Component firmware		11.3	6.3	5.3	5.4	6.7												
Browser extensions		7.2	7.3	6.7														
Asset management		1.1	1.2	1.3	1.4	1.5	1.6	1.8	2.1	2.5	4.1	9.1	12.1	13.1	13.7	15.1	16.1	16.6
Access tokens		4.4	11.5	12.11	15.8	16.3	6.7											

Figure 2: CIS and Mitre Att&ck mapping file

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 86

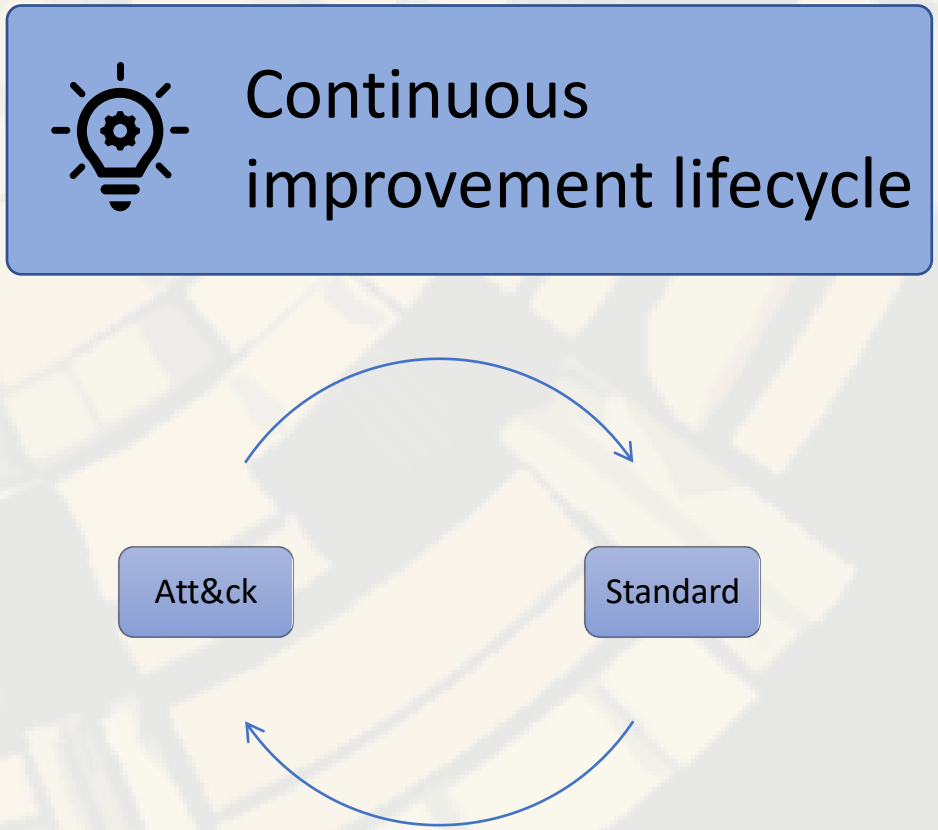


Figure 2: CIS and Mitre Att&ck mapping file

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 86

Design & Methodology – Main Research Question

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 88

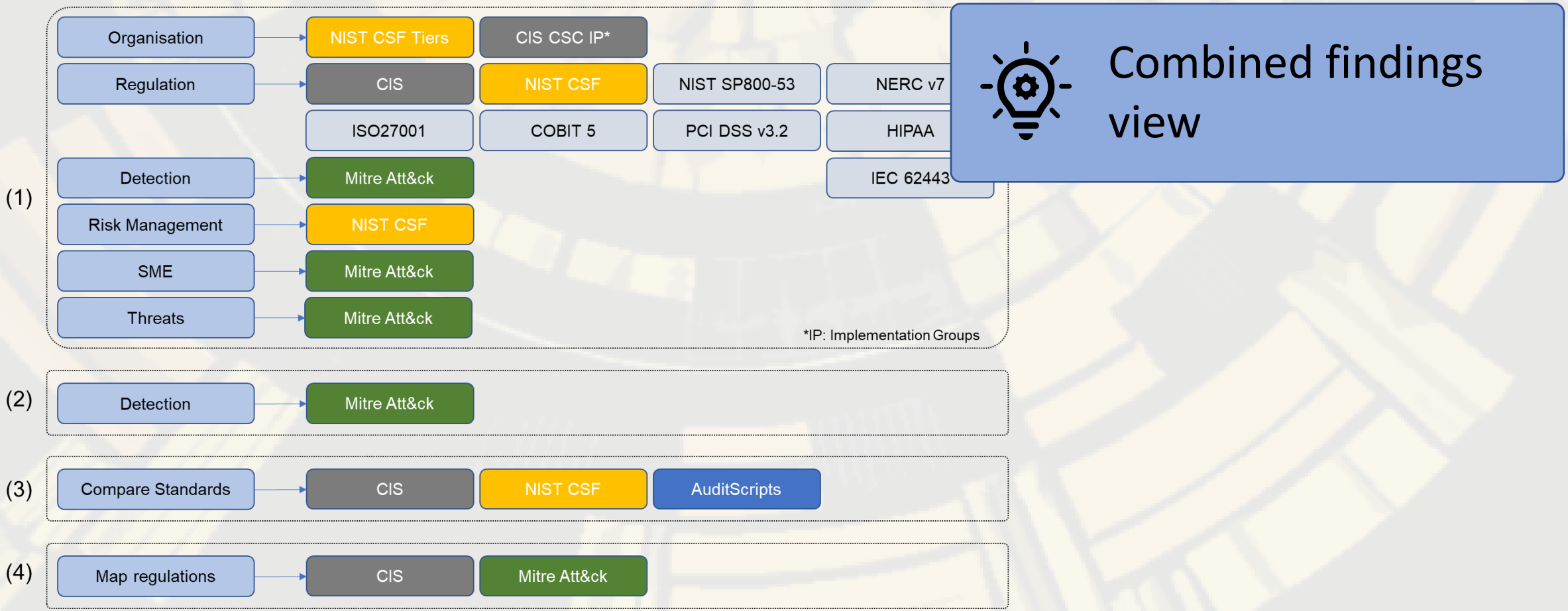


Figure 2: Relationship between all sub-questions

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 88

Design & Methodology – Main Research Question

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 89

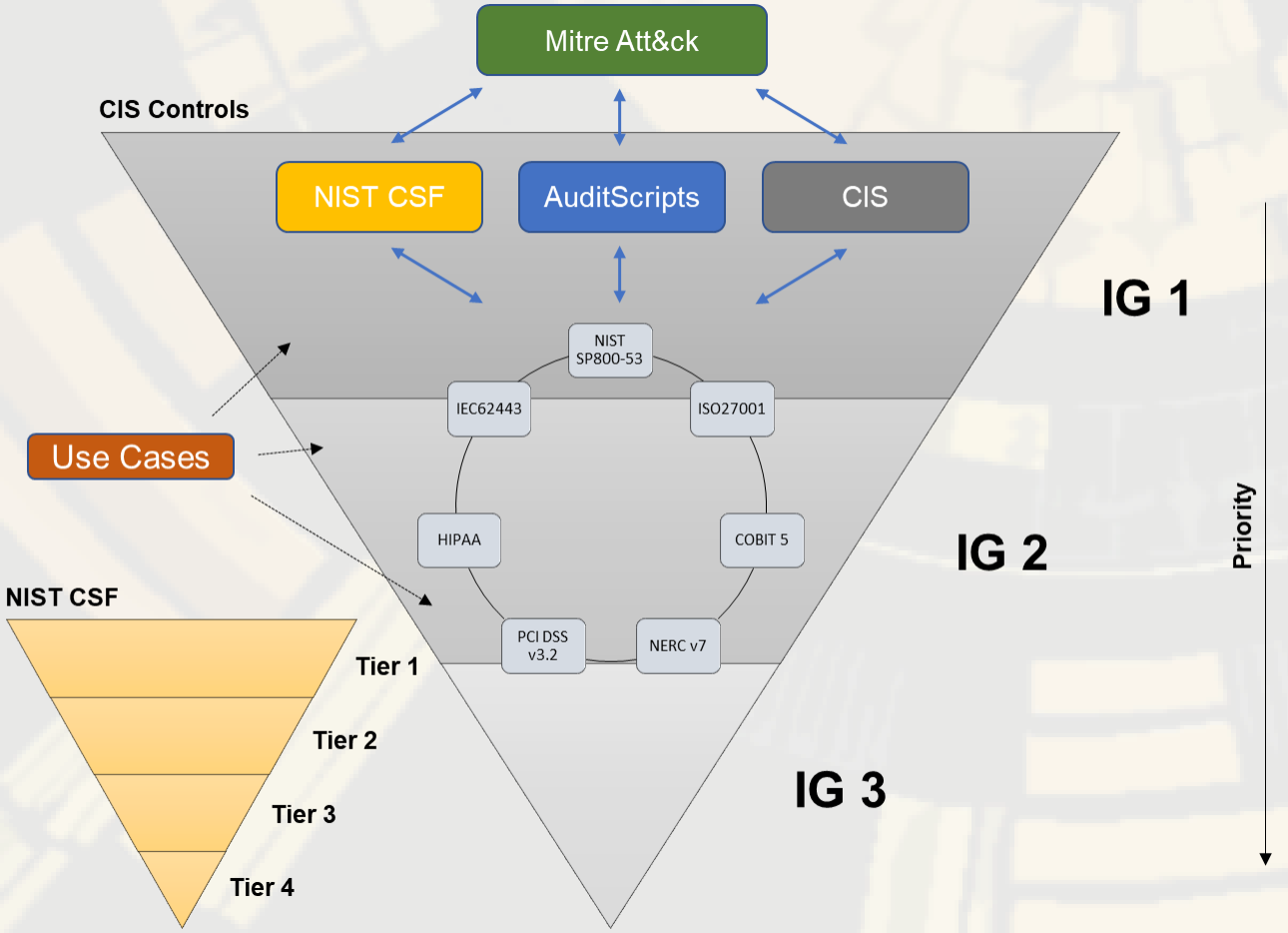


Figure 2: Proposed solution
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 89

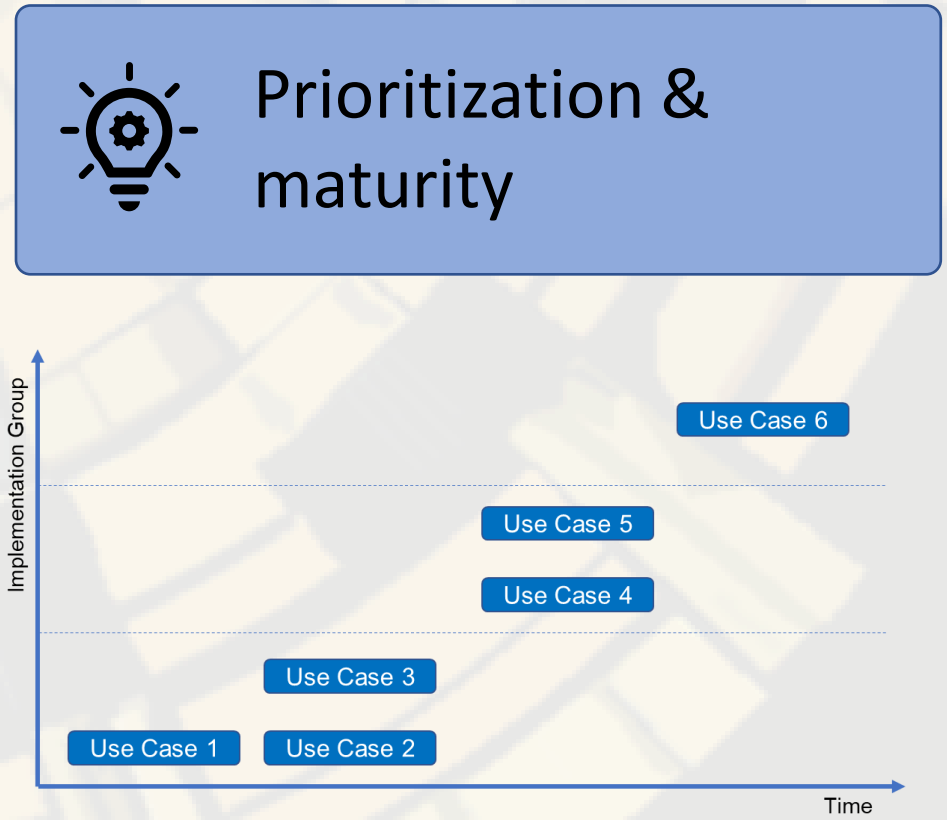


Figure 2: Prioritisation based on framework categorisation of the CIS controls
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 90

Design & Methodology – Main Research Question

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 91

Att&ck Framework features

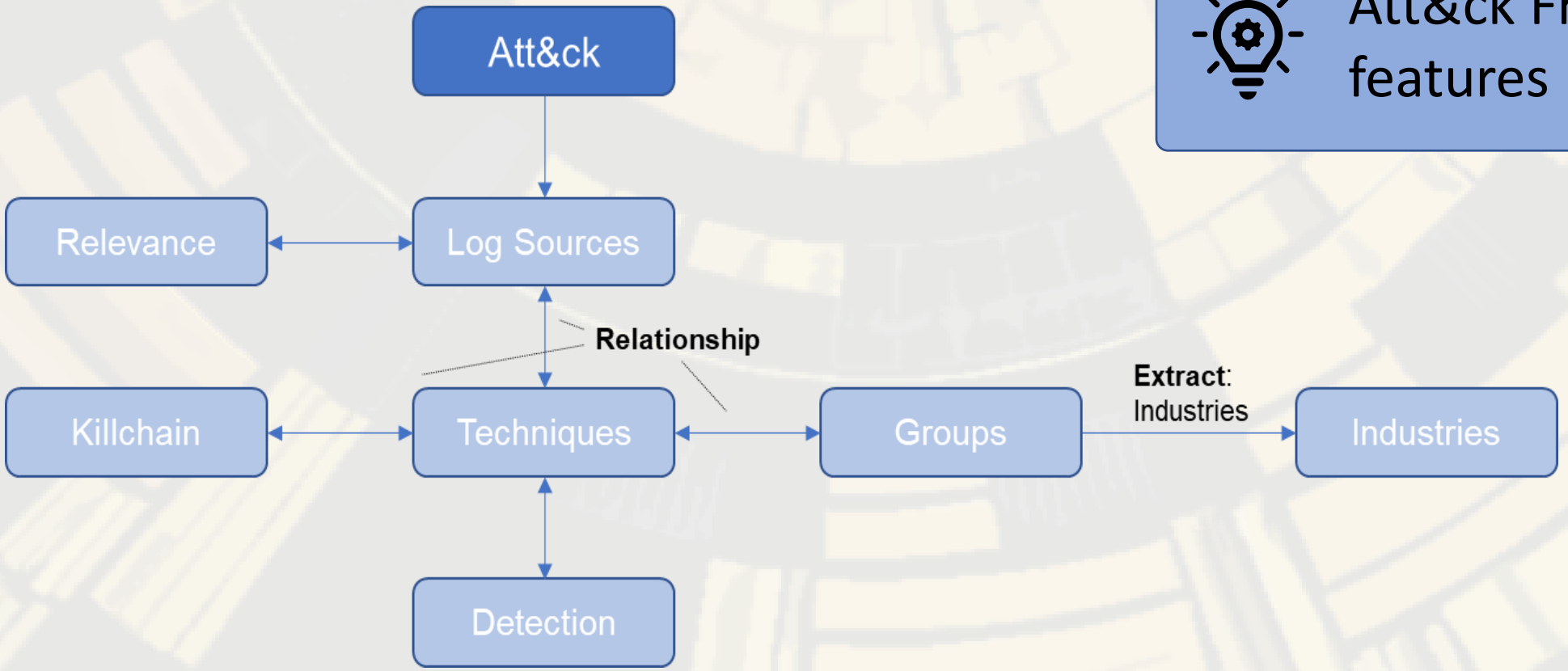


Figure 2: Att&ck data relevant for the mapping
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 91

Design & Methodology – Main Research Question

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 91

Mapping between CIS & Att&ck

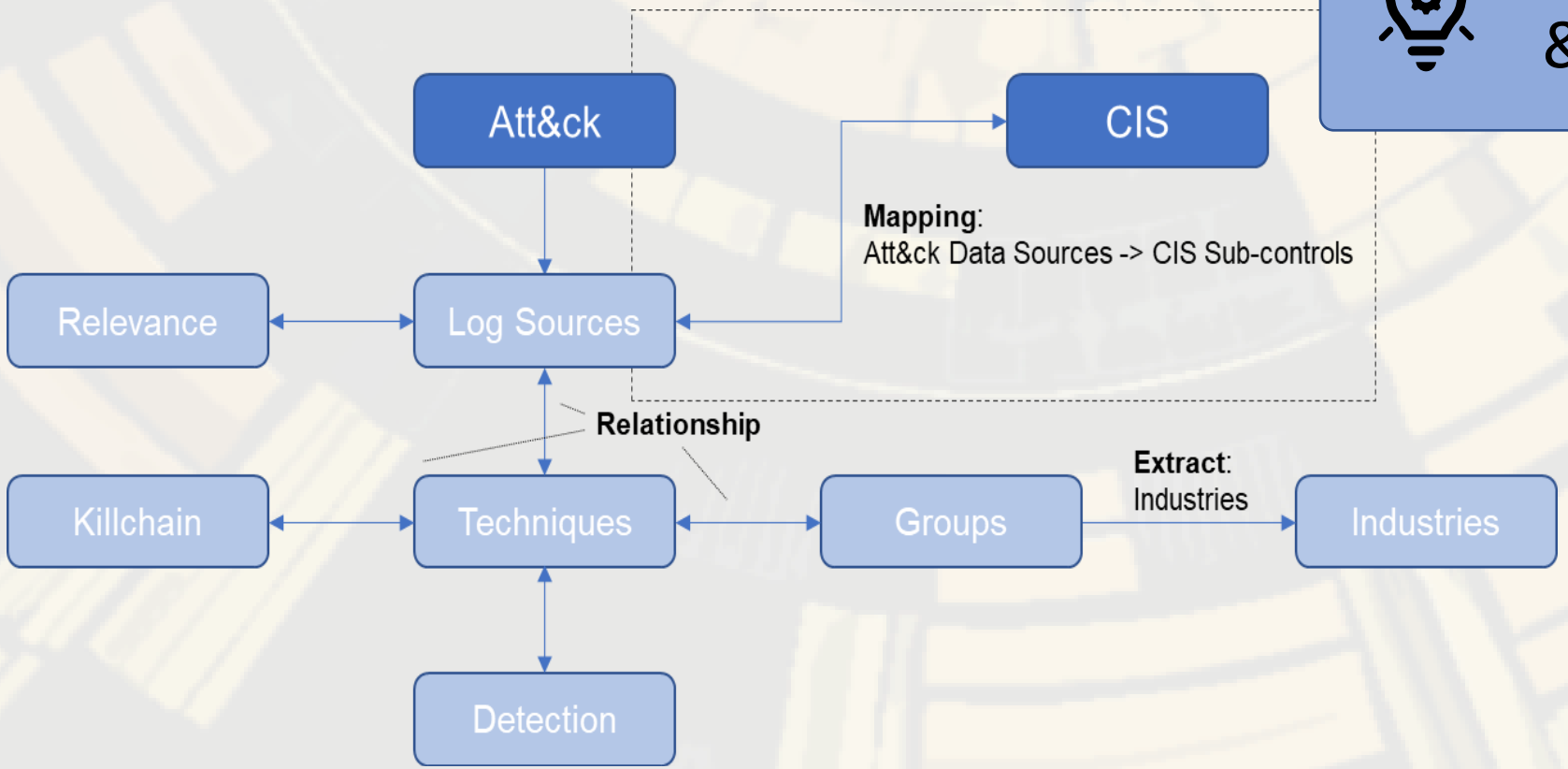
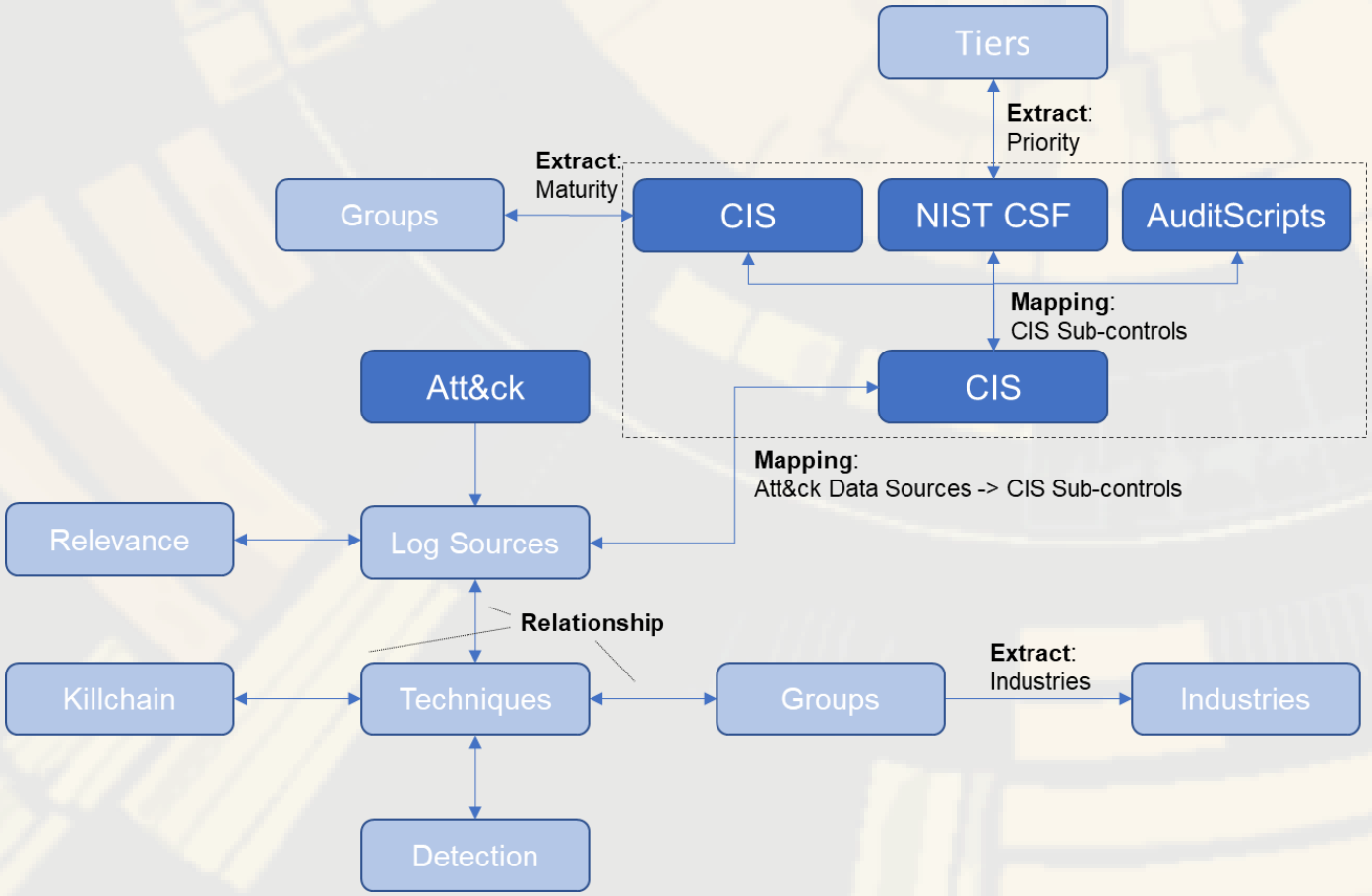


Figure 2: Mapping between Att&ck log sources and CIS sub-controls

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 91

Design & Methodology – Main Research Question

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 92



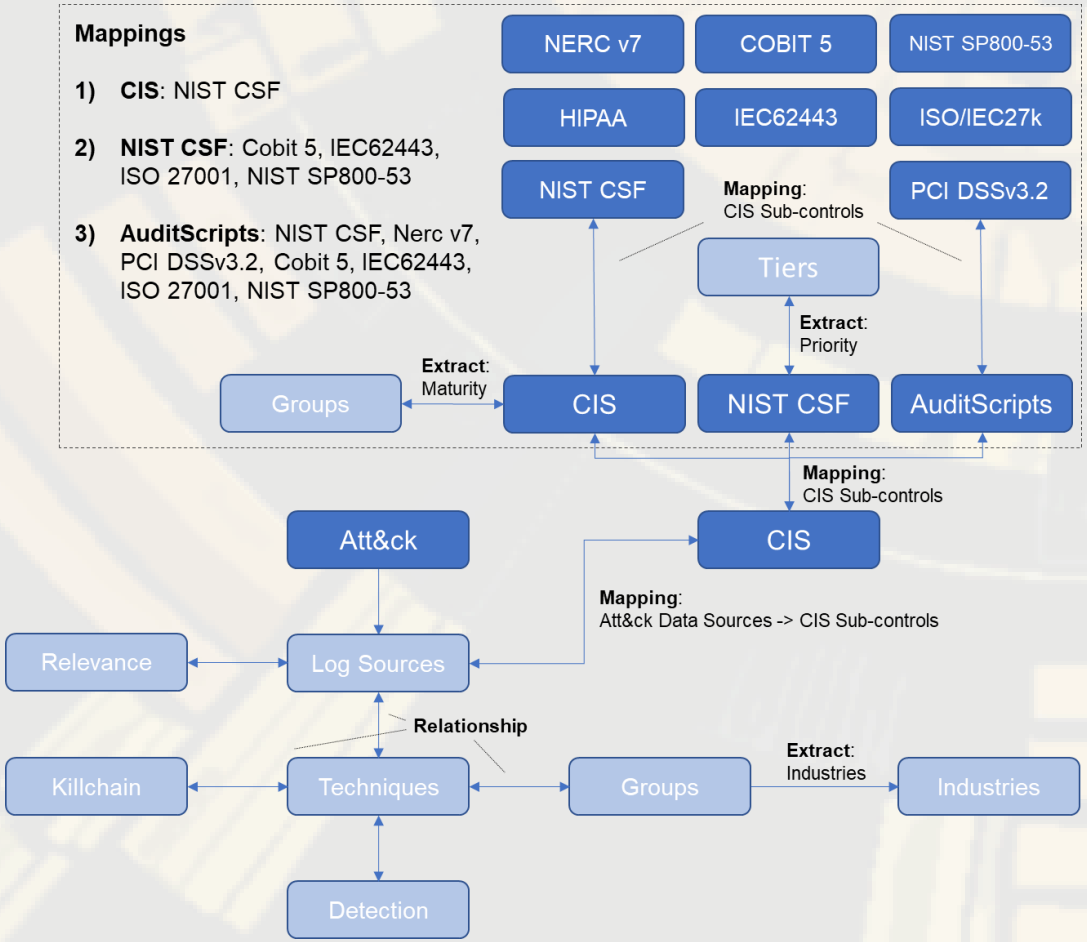
Prioritisation & Maturity

Figure 2: Mapping of CIS sub-controls to the individual mapping files

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 92

Design & Methodology – Main Research Question

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 93



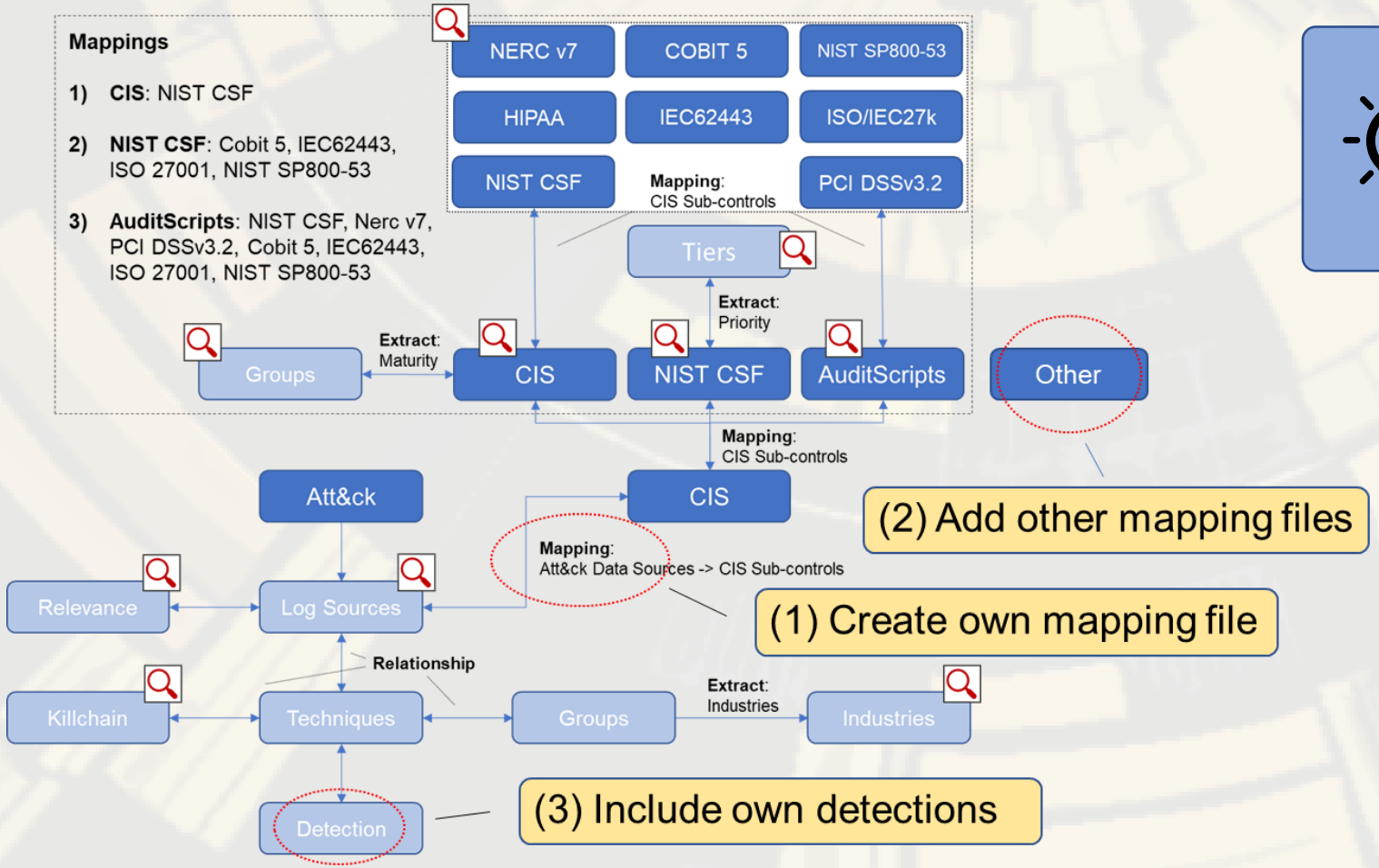
Final mapping content

Figure 2: Mapping overview of all data sets

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 93

Design & Methodology – Main Research Question

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 95



(2) Add other mapping files

(1) Create own mapping file

(3) Include own detections

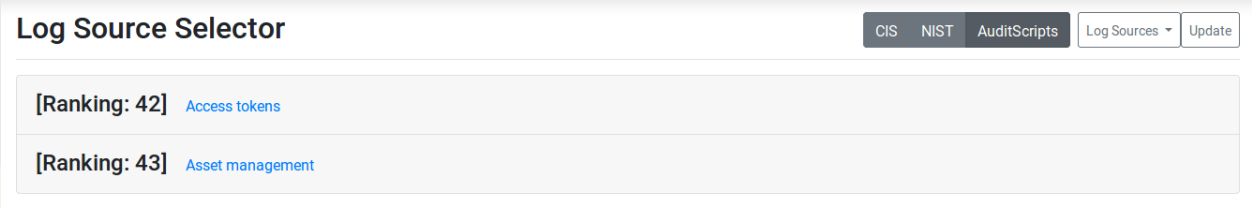
Filters & Improvements

Figure 2: Ease of adjustment of the method

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 95

Design & Methodology – Proof of Concept

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 96



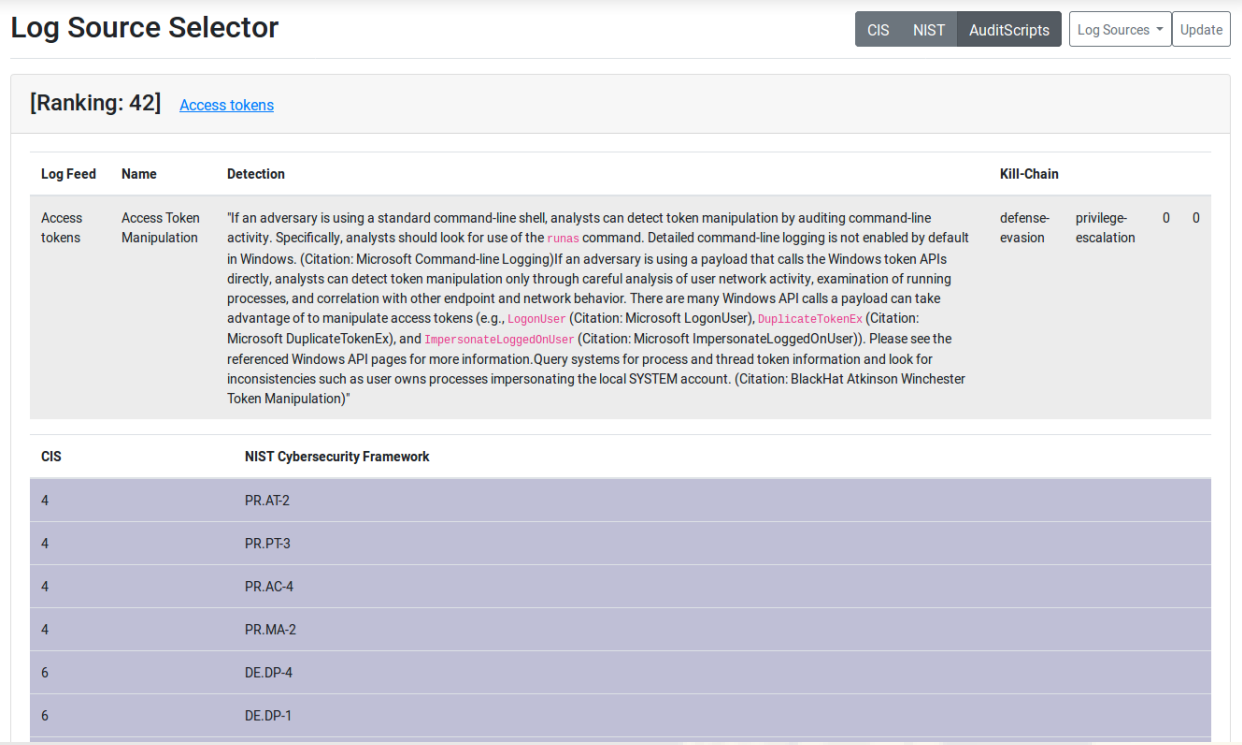


Figure 35: Log source collector and mapping selector
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 96

Selecting log sources:

- Technique
- Detection capabilities
- Killchain
- CIS mapping
- NIST CSF mapping

Figure 36: Detection method and associated NIST CSF sub-controls
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 97

Design & Methodology – Proof of Concept

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 99

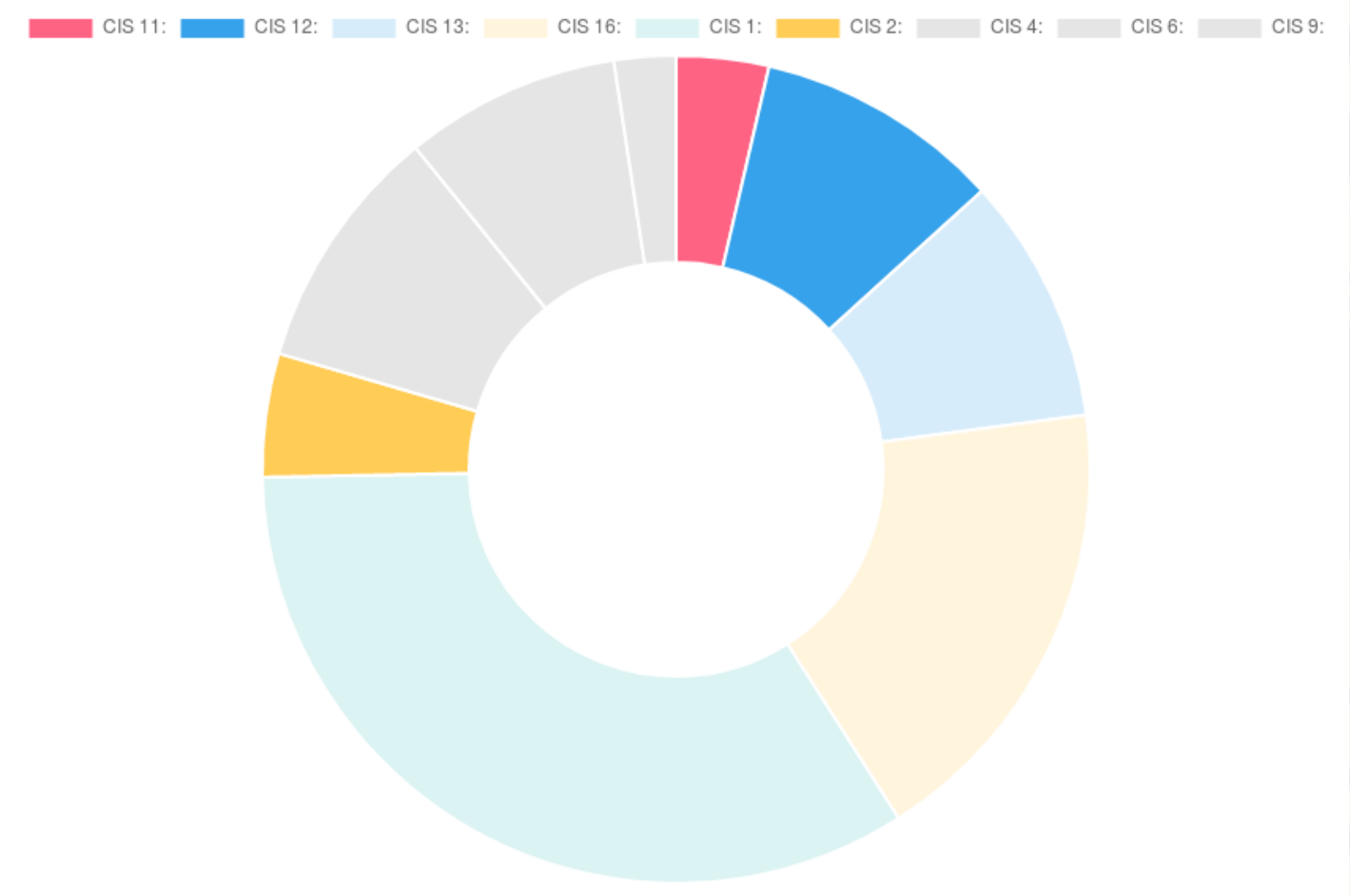


Figure 2: CIS control doughnut chart
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 99

Analysis & Synthesis

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 100

SIEM Use Case Selection

The argument was to find quantitative replacements for the focus areas able to formulate a methodology on how SIEM Use Cases can be selected. The results thereof are direct relationships between the focus areas and standards and frameworks. **With this approach, we can select Use Cases based on frameworks and standards**.

Threats & Detection

The research in chapters 2.2.2 has shown that the **Mitre Att&ck Framework** has proven to be the most effective dataset available.

Standards

If there is a **declaration of which mapping file** is used, then any of the mapping files can be used. It is the same approach as if an organisation defines a standard for their organisation to follow.

Analysis & Synthesis

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 102

Selection

It has been shown in chapter 4.5.2 that such a mapping can be created. The mapping of Att&ck and CIS is done by matching the content of each source logically by terminology. For the remainder with ambiguity or with no direct linkage to sensor technology, the whole framework description and the attack data set had to be compared against each other.

Main Research Question

This research has shown that it is possible to have a unified approach in using SIEM Use Case focus areas necessary for their selection and combine them with the relevant cybersecurity standards and frameworks. The result is a flexible best practises solution allowing for various parameters to be configured to receive a list of applicable SIEM Use Cases.

Conclusion

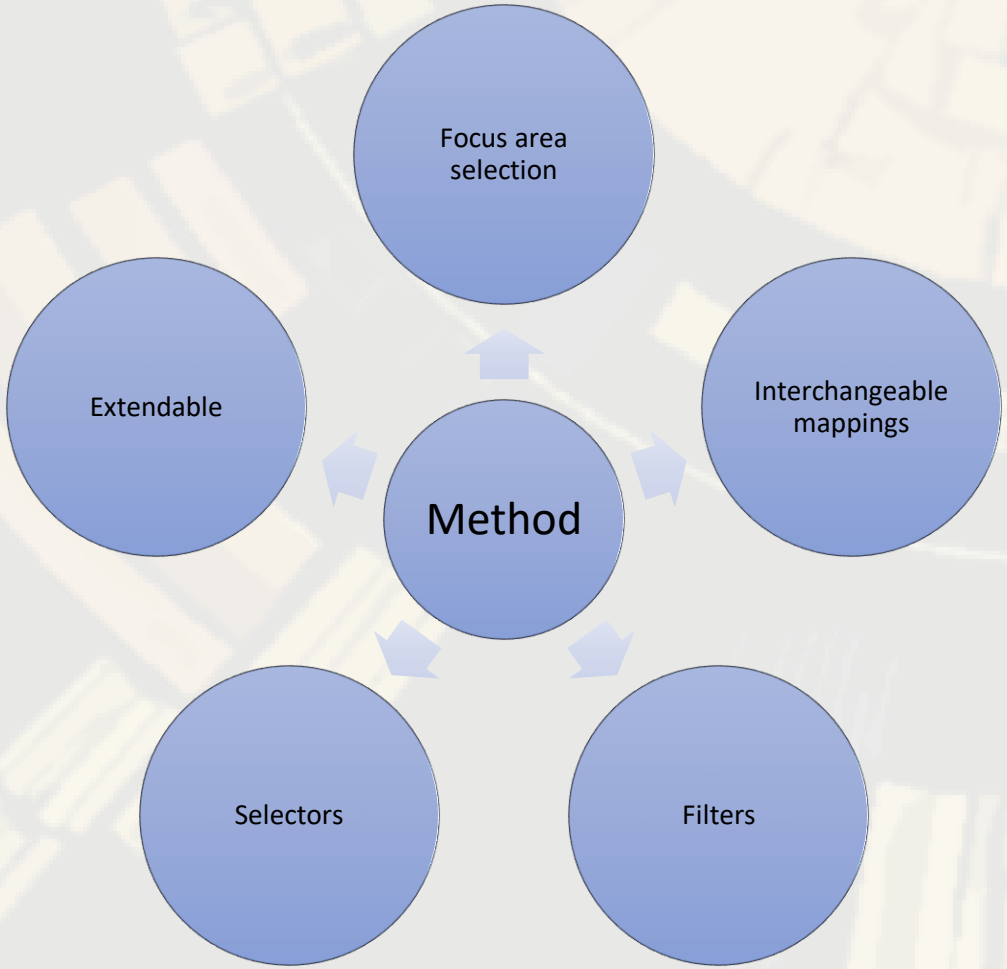
Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 103

The research has shown that **it is possible to have a unified approach** in using SIEM Use Case focus areas necessary for their selection and combine them with the relevant cybersecurity standards and frameworks.

- The result is a **flexible methodology** allowing for various parameters to be configured to receive a list of applicable SIEM Use Cases.
- With moving the **detection capability** of an organisation back into the focus, we can break down the goals based on the data gathered.
- **None of the existing parameters was subdued** or marginalised with this approach, and it still can be added if required.
- At the centre is still a **robust cybersecurity program** driving the organisational needs, but it will be supported with qualified data from a relevant threat source able to assist in formulating a roadmap of rolling out detection capabilities.
- It answers the questions **of what is needed** to be able to detect the cybersecurity threats trageting the organisation.

Flexibility of the method

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 103



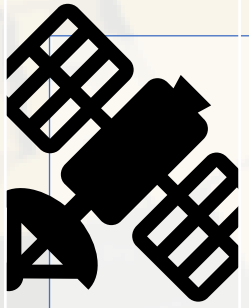
The presented method is very diverse and highly flexible model to select SIEM Use Cases.

Further Research

Source: Methodology to select Security Information and Event Management (SIEM) Use Cases - Page 103

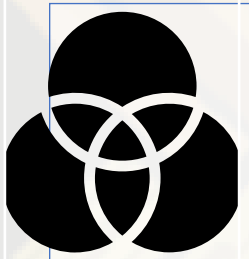
More Use Cases

- Incorporation of other SIEM Use Case resources such as SIGMA[1] or SOCPrime[2]. A guide could be provided also to include self-developed SIEM Use Cases and how to map them to the Att&ck Framework.



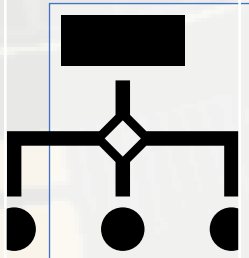
Public Portal

- Further development of the application to upload risk assessment results of one of the supported frameworks and then provide an overview of which SIEM Use cases to deploy in which prioritisation, the required log sources, the association to the other standards and the statistical overview of CIS, kill-chain and NIST CSF functions.



1. Att&ck Framework enhancement

- Reach out to Mitre for a suggestion to include business-relevant information such as discussed in chapter 4.3. Increasing the reach of the Framework in order to protect organisations must be a goal of every cybersecurity practitioner.



2. Att&ck Framework enhancement

- Reach out to Mitre to suggest the mapping to CIS. The impact of a precise mapping is much more significant than done by an individual. If the mapping can help to drive the adoption rate, then it is a win for all.

[1] https://github.com/Neo23x0/sigma [2] https://my.socprime.com/en/tdm/

Thank you!