
ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group
A new approach to select SIEM Use Cases
swiNOG #36 – November 14th 2019
persistent security in a changing world

Speaker Introduction: Pascal Imthurn

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

- Head Cyber Defense Services
- 20 years of experience in IT Sec
- Most important milestones:
  - Open Systems: Security Architect
  - UBS: Global Head of SOC
  - Various: Linux firewall developer, reverse engineer, threat analyst

Key learnings

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

- Methodology to select SIEM Use Cases
- Measure coverage of your SIEM Use Case regarding the MITRE Att&ck Framework and various standards
- Guidance on the selection of the most security relevant log feed

Agenda

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

1. Problem Statement
2. SIEM Use Case Definition & Drivers
3. Mitre Att&ck Framework
4. SIEM UC Selection Methodology
5. Most useful data log sources for threat detection
6. Conclusion and Problem Statements solved

Set the scene (definitions, namings)

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

SOC: **S**ecurity **O**peration **C**enter → **People**

SIEM: **S**ecurity **I**ncident & **E**vent **M**anagement → **Technology**

SIEM Use Cases: Attack pattern to detect and its req. activities → **Process**

Log Feed: Type of log source (e.g. FW)

Log Source: Log generating asset (e.g. FW01)

EDR: **E**ndpoint **D**etection & **R**esponse

MSSP: **M**anaged **S**ecurity **S**ervice **P**rovider

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

Problem Statement

ISPIN Cyber Defense Services

1

Problem Statements

- Which ***SIEM use cases*** do I need to implement to achieve a ***good threat detection*** maturity? - how do I measure the threat detection maturity?
- Which ***log sources*** are ***important*** to establish a ***reliable detection coverage*** from an early stage? – how do I measure the threat detection coverage?
- How can existing ***cybersecurity standards*** and ***frameworks*** be mapped to ***threats and detection capabilities?***

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

SIEM Use Case Definition & Drivers

2

ISPIN Cyber Defense Services

What is a SIEM Use Case?

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

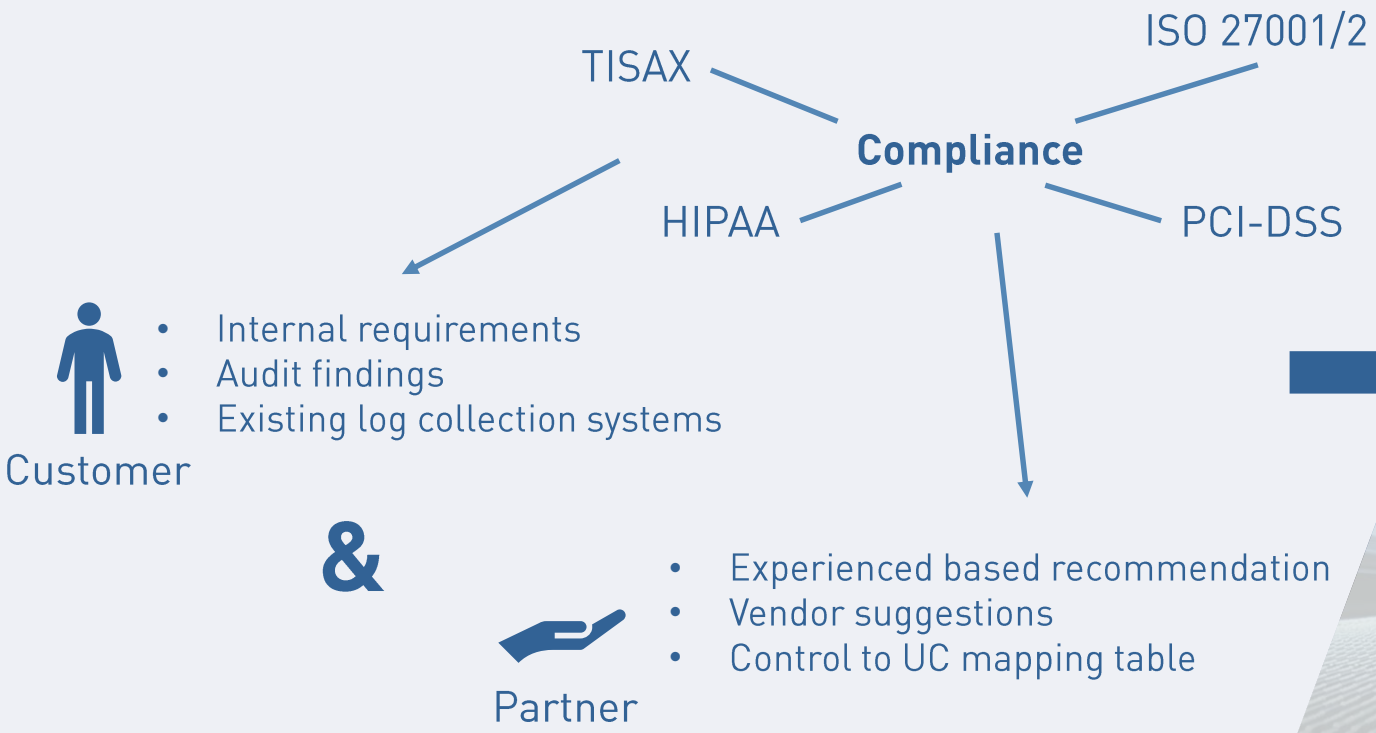
- *Specific condition or event (usually related to a specific threat) to be detected or reported by the security tool"* (Gartner, How to Develop and Maintain Security Monitoring Use Cases, 2016)
- **"Methodology used by the SOC team to identify and organize technical and organizational requirements for detection and response to specific threats."** (Perniola & Gray)

Objective → Threat → Stakeholders → Data Requirements → Logic → Testing & Tuning → Priority → Output

- Improves Effectiveness of SOC by targeting resources.
- What we want to Defend against.
- Who will be involved? Analysts, IT OPS, HR, internal Security, Law Enforcement Units, MSSPs
- The raw Log/Packet/Flow/Endpoint Data sources that are required to be able to detect our Threat
- Parsing of events and correlating, aggregating information out of events → rules
- How we know the Logic will produce a (reliable) alert and related tuning activities required.
- Provides guidance to SOC Analysts dependent upon policies and business requirements → criticality of assets
- Alert, Remediation → Dashboard and relating events for deep analysis by Analysts and remediation activities

Traditional SIEM Use Case Drivers & Selection

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group



Use case mapping:
Compliance → Use Case → Log Feeds → Log Sources

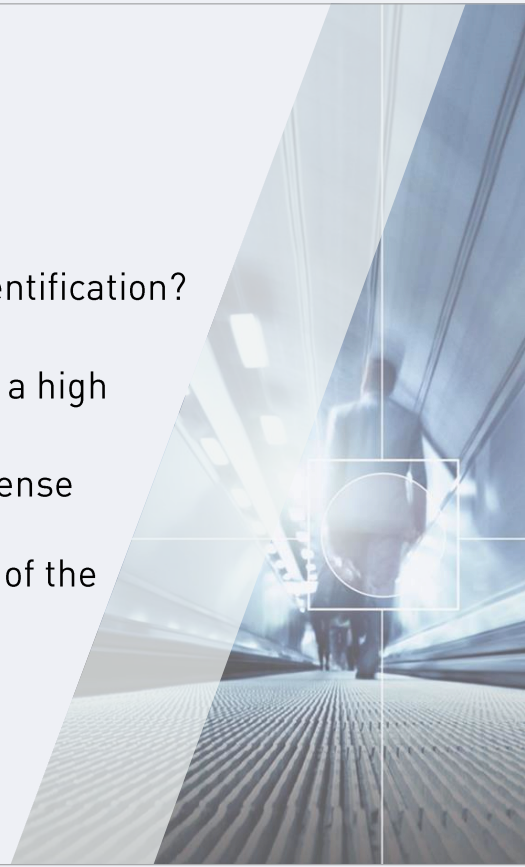
ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

VDA-ISA	ISO 27k1	Use Case	Log Feeds	Log Sources
…	…	…	…	
8.3	A8.3.1 A8.3.2 A8.3.3	• Devices (workstations, servers) with high event rates • Excessive Database Connections • Excessive Firewall Denies from Single Source • Reconnaisance activities using ICMP Packets. • …	Endpoint Security, Domain Controller, Firewall, IDS, Proxy, Database, …	Server01, Server03, FW02
…	…	…	…	
9.1	A9.1.2	• Inbound and Outbound communication of internal assets with specific blacklisted countries/regions • Remote Access from a specific Country or Region. • Long Duration Flow Involving a Remote Host. • …	Endpoint Security, Firewall, IDS, Proxy, DNS, …	Client04, Proxy05, DNS07
…	…	…	…	
12.	A.12.7.1 A.18.2.3	• Potential Botnet Connection. • Potential Connection to a Known Botnet C&C (Command and Control) Server. • Successful Inbound Connection from a Known Botnet C&C (Command and Control) Server. • …	Endpoint Security, Firewall, IDS, Proxy, …	Client09, Proxy10, IDS05
….	…	…	…	

Traditional SIEM Use Case Evaluation: Challenges

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

- SIEM use cases evaluation based…
  - on compliance framework:
    Which ones? Are 20 or 40 SIEM use cases enough?
  - on already existing log sources:
    Are already collected log feeds the adequate driver for SIEM use case identification?
  - on achievement to establish a high security detection maturity:
    Which prioritization to implement the SIEM use cases is required to have a high security detection maturity from day one?
  - on less log sources/log volume as really needed to keep SIEM volume license affordable:
    Do I have to integrate all log sources to have a good coverage regardless of the SIEM license fee?



ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

Mitre Att&ck Framework

ISPIN Cyber Defense Services

3

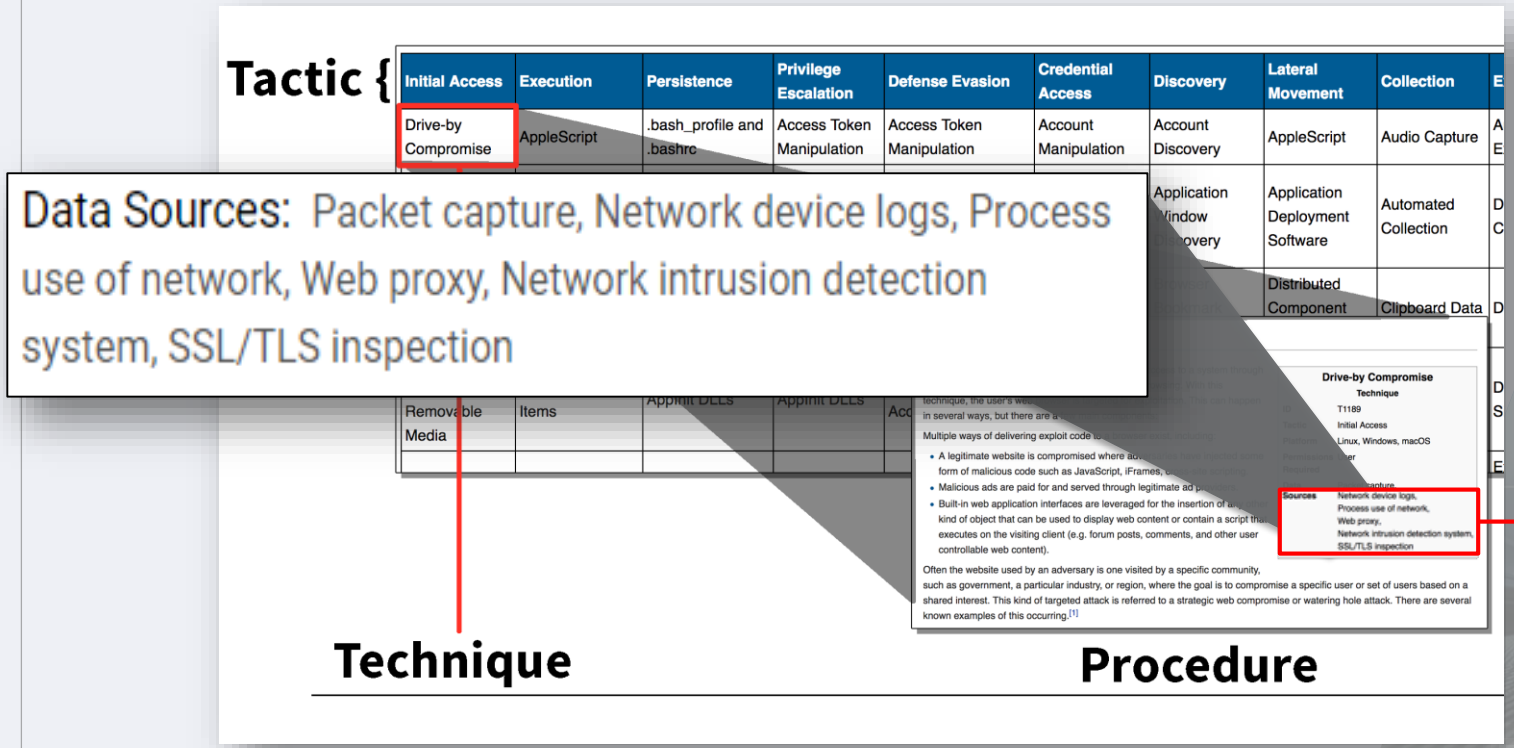
MITRE ATT&CK Framework

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

*"**MITRE**'s Adversarial Tactics, Techniques, and Common Knowledge (**ATT&CK**) is a curated **knowledge base** and **model** for **cyber adversary behavior**, reflecting the various phases of an **adversary's attack lifecycle** and the platforms they are known to target",*

Strom B. et al. (2018)

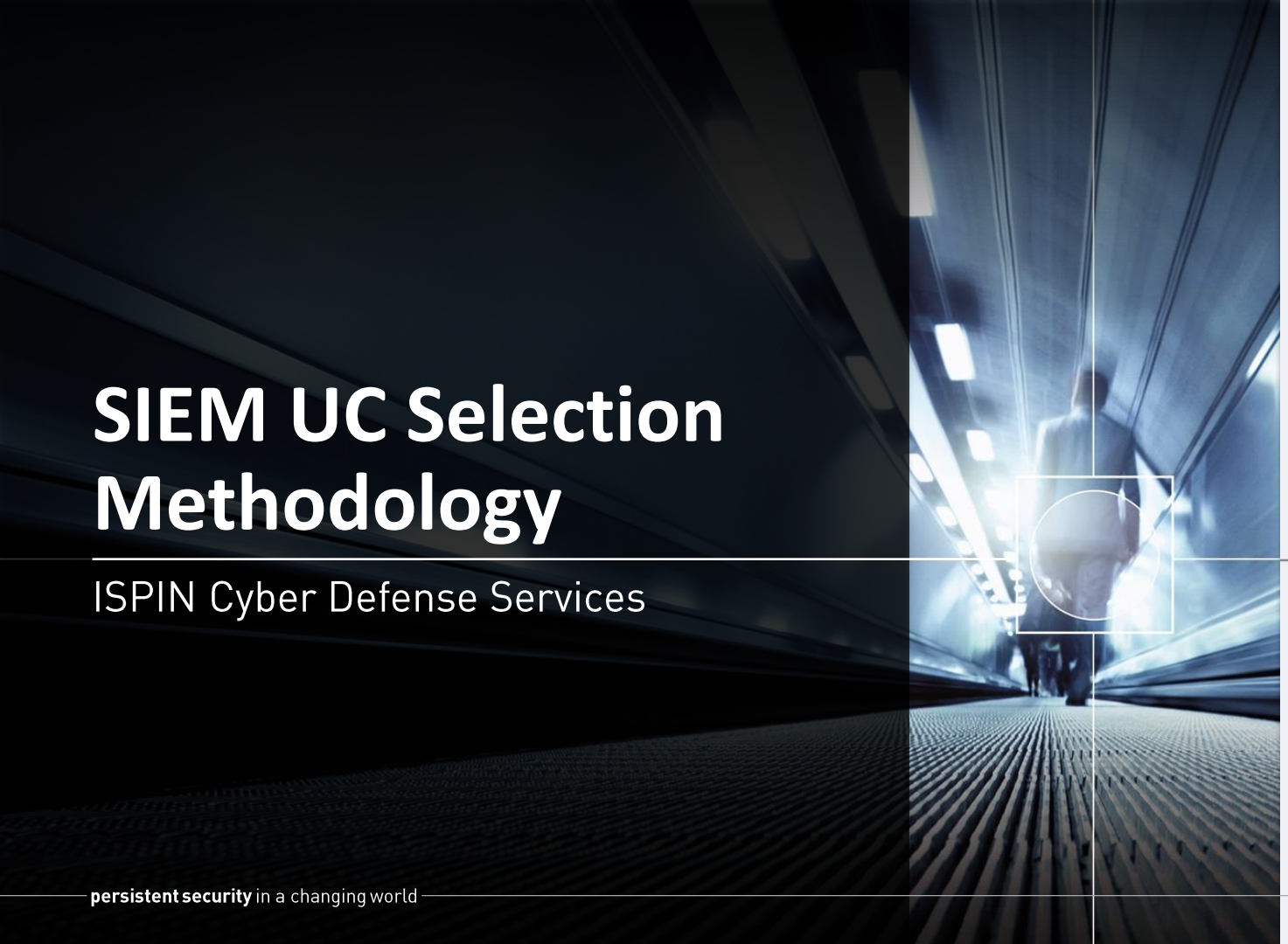
MITRE ATT&CK Framework: Terminology



MITRE ATT&CK Framework: Why is it useful?

- It combines the worlds ***intelligence*** and ***know-how*** to ***detect*** and ***prevent*** the most prolific public ***cyber attacks***. It will never be 100% complete but it is to date the most accurate threat database.

- The framework can be used to:
  - classify attacks
  - assess risk posture
  - identification of gaps in detection
  - research attacks and detection capabilities
  - map attacks to groups
  - prioritize rollout of detection measures based on industry



ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

SIEM UC Selection Methodology

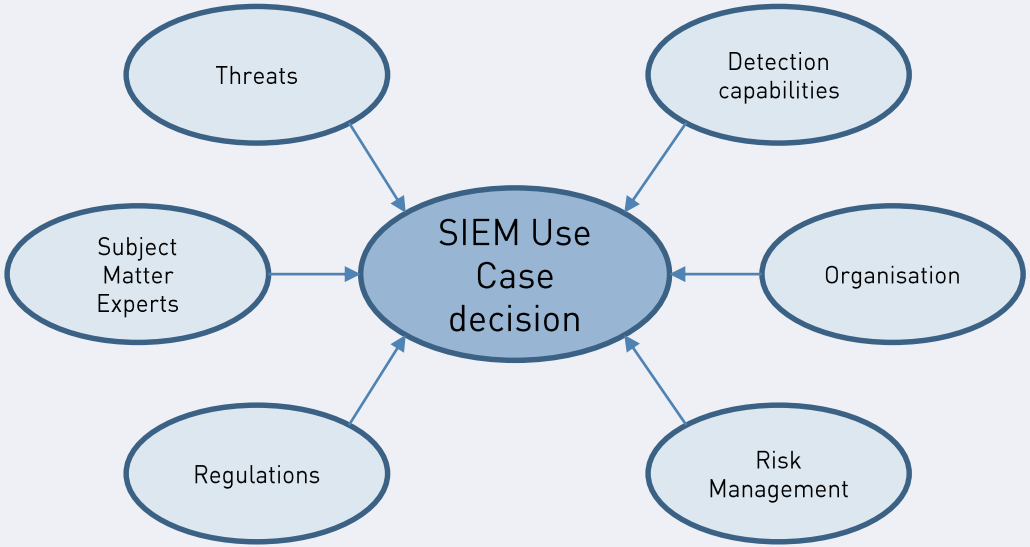
ISPIN Cyber Defense Services

4

SIEM UC Selection: Focus Areas & Decision Galaxy

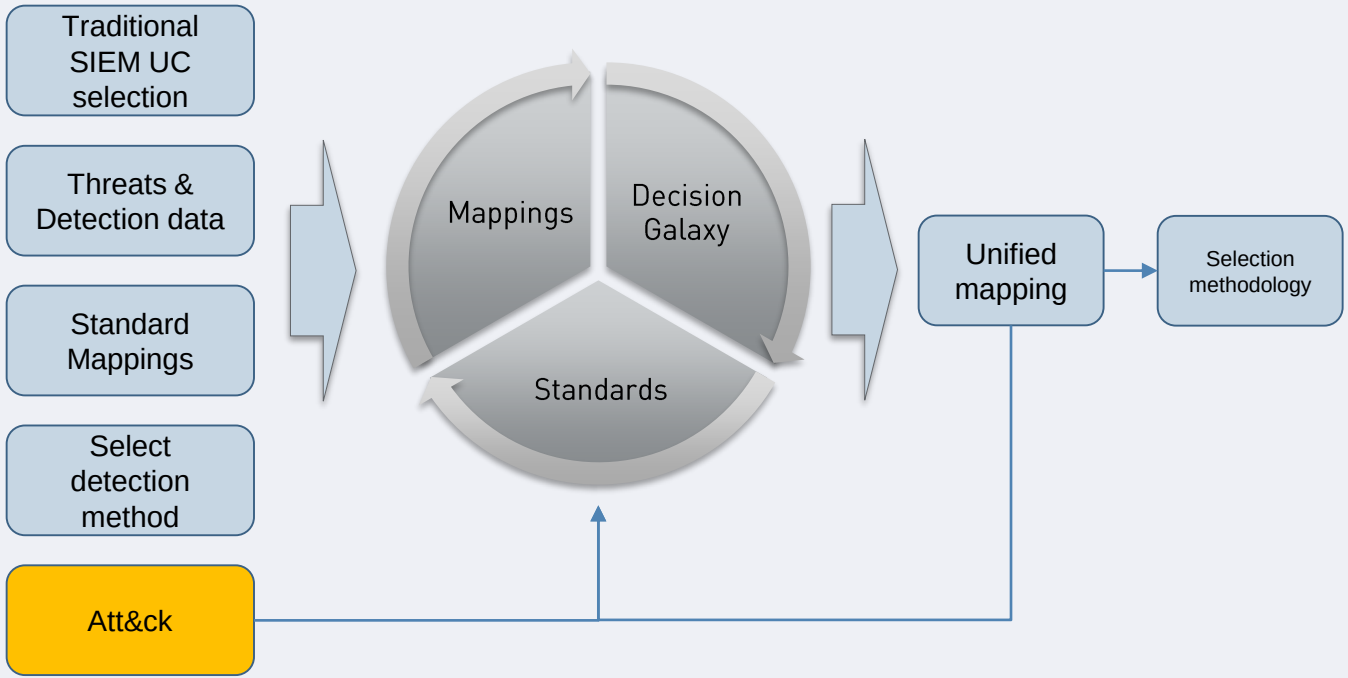
ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

The condensed form of slide 11 provides us with following focus areas / decision galaxy on selecting SIEM Use Cases.



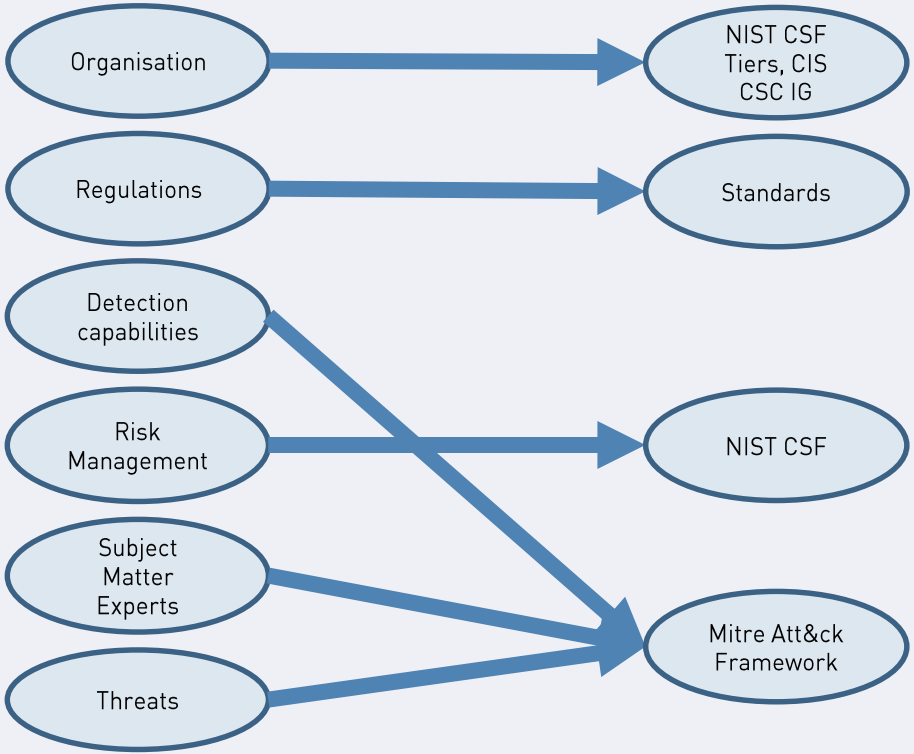
Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: How to improve?



Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Simplification



Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

Draw experience from cyber security frameworks

Your “goto” standards

Do you have to re-invent the wheel?

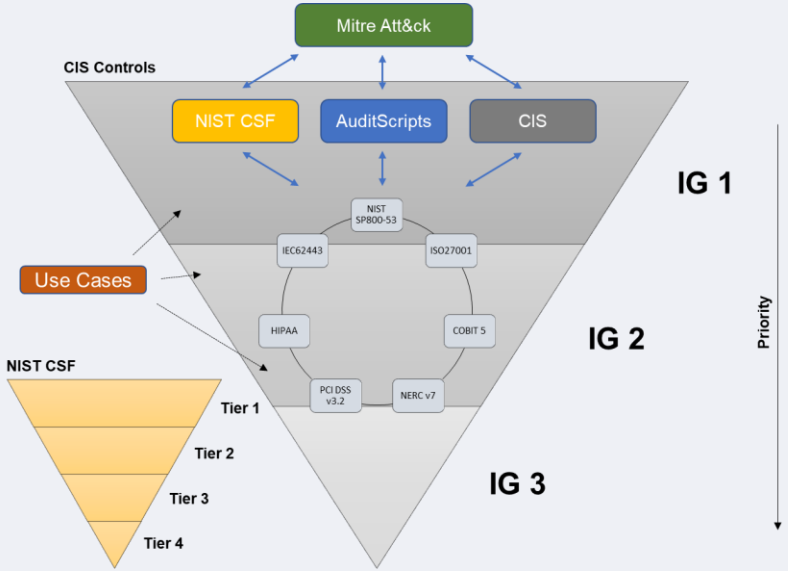
Cyber Security component to your risk management

Not every company has them

Attack vectors & targets

SIEM UC Selection: Prioritization & Maturity

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group



Implementation Groups and the Tiers allow for roadmap design of SIEM UC

Organisation

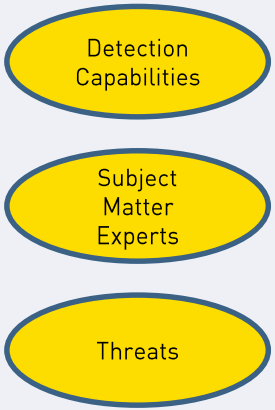
Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Threat Detection

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

→ 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.



Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Regulations & Risk Management

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

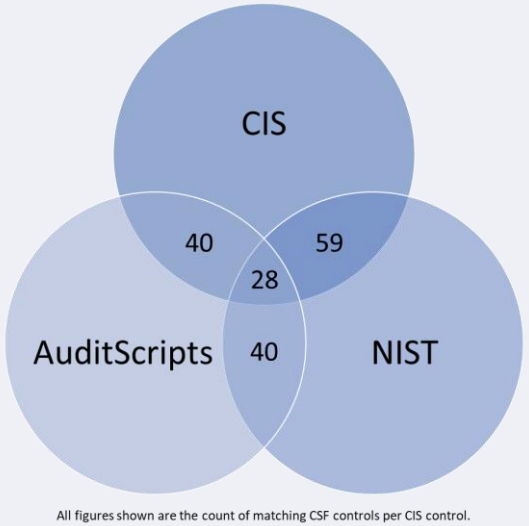
Standards	CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443
Risk Management	The NIST Cyber Security Framework enjoys an increased adoption rate (Swiss Minimal ICT Standard)

Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Standards Mappings

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

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



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

⇨ **The organisation simply declares which mapping file has been used**

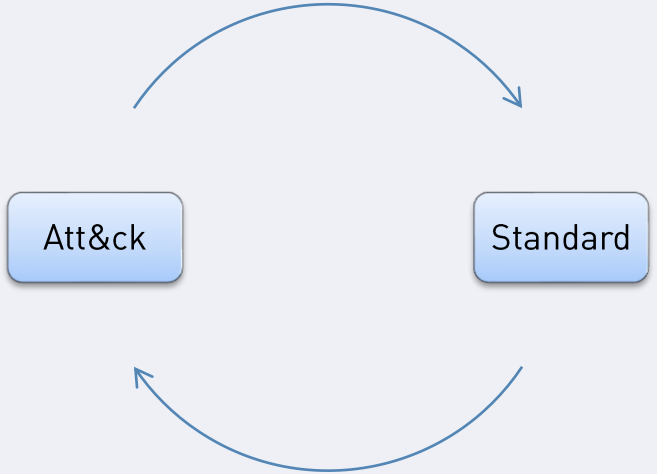
Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Map Attack Framework to CIS

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

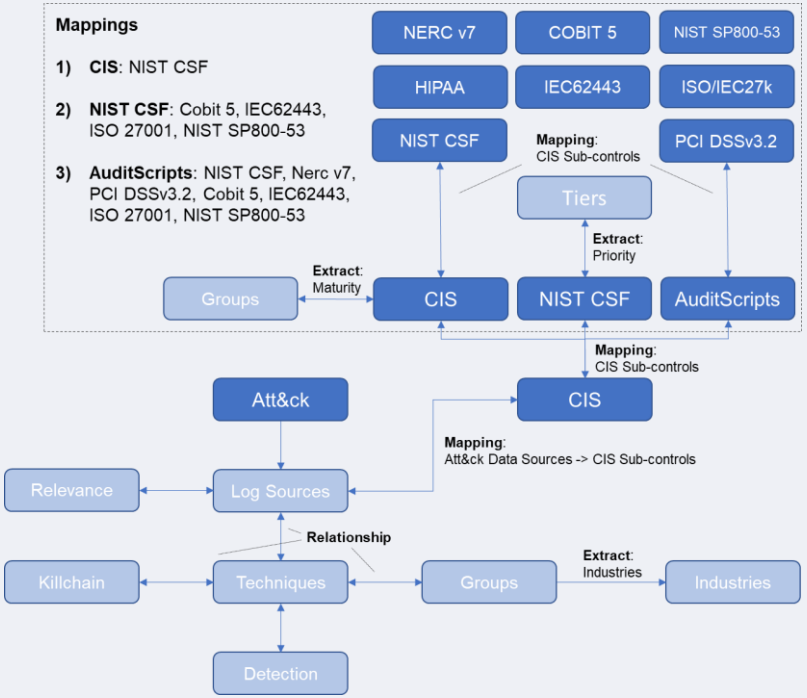
Attack		CIS Subcontrol																
Process monitoring	Detection	8.3	6.2	6.3	2.8	2.9	6.7											
File monitoring		14.9	5.5	5.3	6.3	6.7	4.8											
Process command-line parameter		8.8	2.9	14.9	6.3	6.7												
API monitoring		8.8	14.9	6.3	5.3	5.4	6.7	11.3	8.3	2.8	5.5	2.9	16.6	6.2				
Process 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											

This is the last step to a selection methodology. The combination of CIS with the Mitre Attack Framework



Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Final mapping content

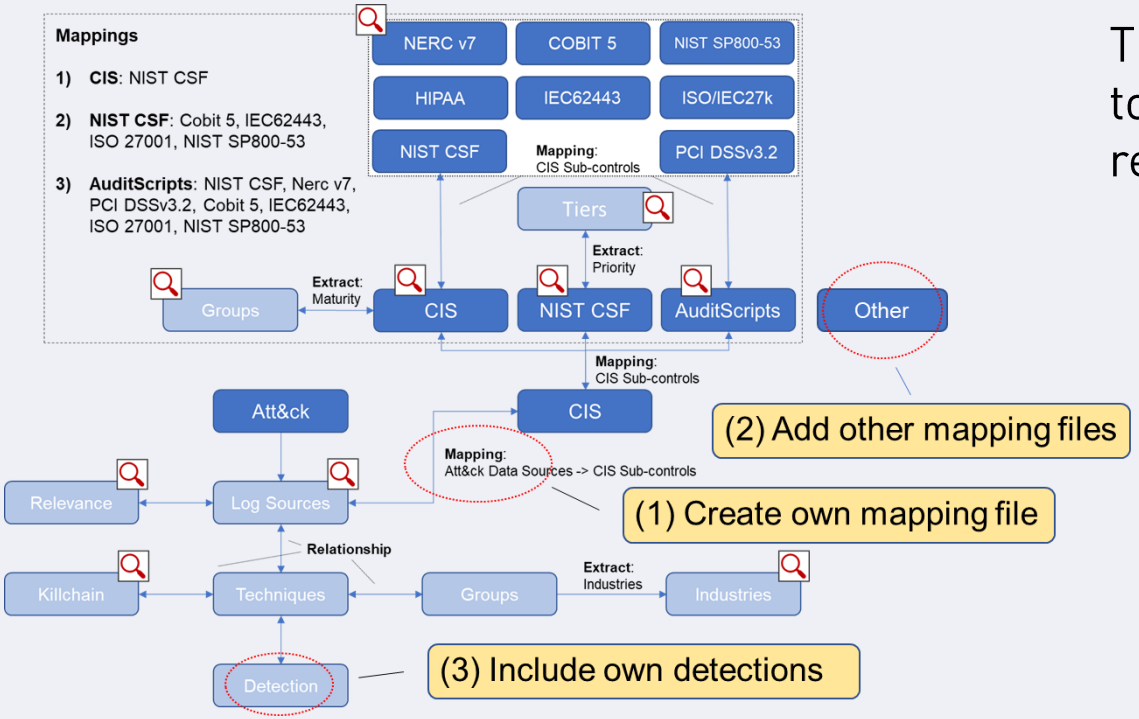


All is combined and we have unified approach to select SIEM Use Cases based on following criteria's:

- Organisation
- Regulations
- Detection
- Risk Management
- Subject Matter Experts
- Threats

Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Improvement



This approach is extensible to accommodate individual requirements.

The important part is, that it prevails as a repeatable and measurable selection process for SIEM Use Cases.

Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

SIEM UC Selection: Improvement

There you go, a repeatable methodology to select SIEM Use Cases.

- 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.

Source: Imthurn P. (2019); Methodology to select Security Information and Event Management (SIEM) Use Cases

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

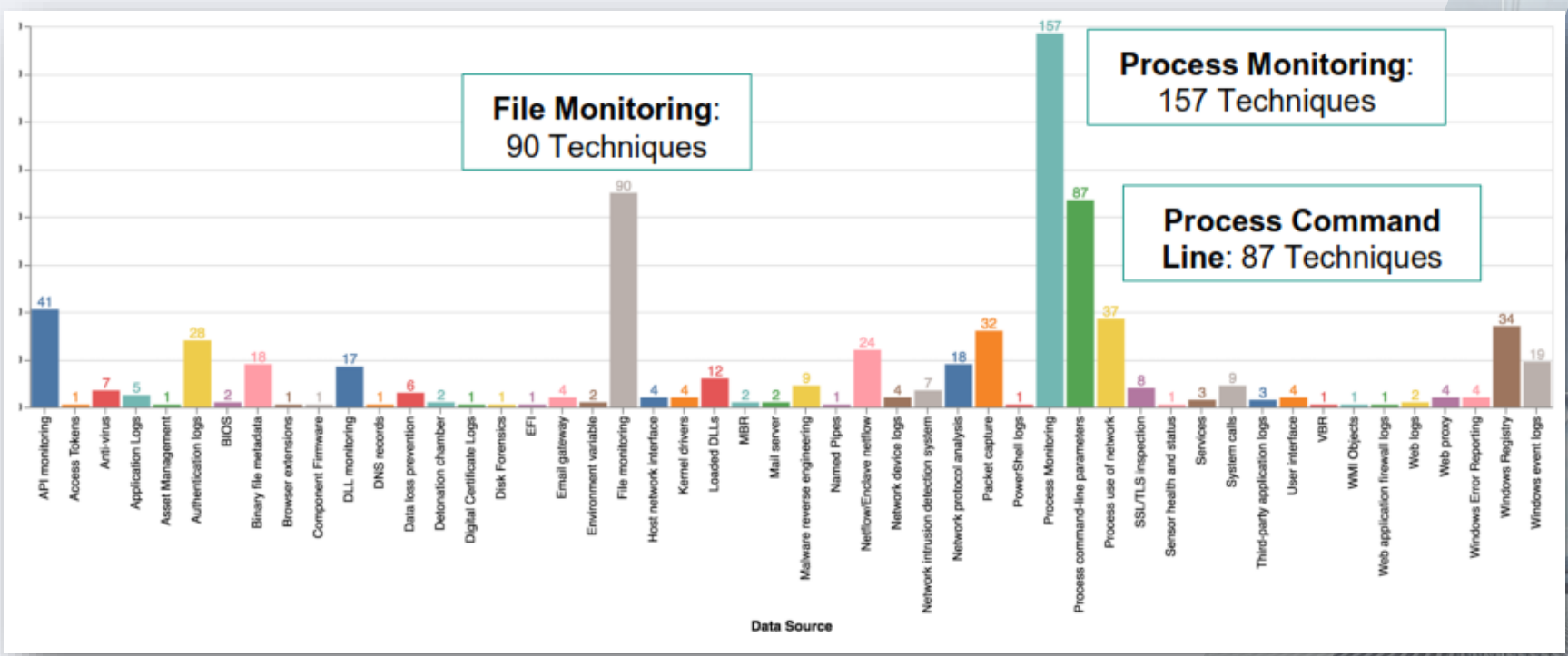
Most useful data log sources for threat detection

ISPIN Cyber Defense Services

5

MITRE ATT&CK Framework:
244 techniques clustered to 50 data sources

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group



Source: Rodriguez R. et al. (2018), MITRE ATT&CKcon 2018: Hunters ATT&CKing with the Data

MITRE ATT&CK Framework:
Data Sources mapped to log feed (ranking based on techniques included)

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

Rank	Data Source	Log Source/Module
1	Process monitoring	Endpoint Detection & Response Logs (Client, Server)
2	File monitoring	Endpoint Detection & Response Logs (Client, Server)
3	Process command-line parameters	Endpoint Detection & Response Logs (Client, Server)
4	API monitoring	Endpoint Detection & Response Logs (Client, Server)
5	Process use of network	Endpoint Detection & Response Logs (Client, Server)
6	Windows Registry	Endpoint Detection & Response Logs (Client, Server)
7	Packet capture	Endpoint Detection & Response Logs (Client, Server)
8	Authentication logs	User Directory Logs
9	Netflow/Enclave netflow	Endpoint Detection & Response Logs (Client, Server) Network Analyzer Logs
10	Windows event logs	Endpoint Detection & Response Logs (Client, Server)
		.....
		.....
		.....
		.....
		.....
		.....
50	WMI Objects	Endpoint Detection & Response Logs (Client, Server)

- Analysis yields ***endpoint*** as ***log feed*** as the ***most relevant***.
  - 7 out 10 topmost data log sources have endpoint as log feed identified.
  - 29 out of 50 data log sources are endpoint relevant.
  - The top first 4 data sources are endpoint relevant:
    - Data source “Process monitoring” contains 157 attack techniques (64%).
    - Data source “File monitoring” contains 90 attack techniques (37%).
    - Data source “Process command-line parameters” contains 87 attack techniques (36%).
    - Data source “API monitoring” contains 41 attack techniques (17%).

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

Conclusion and Problem Statements solved

ISPIN Cyber Defense Services

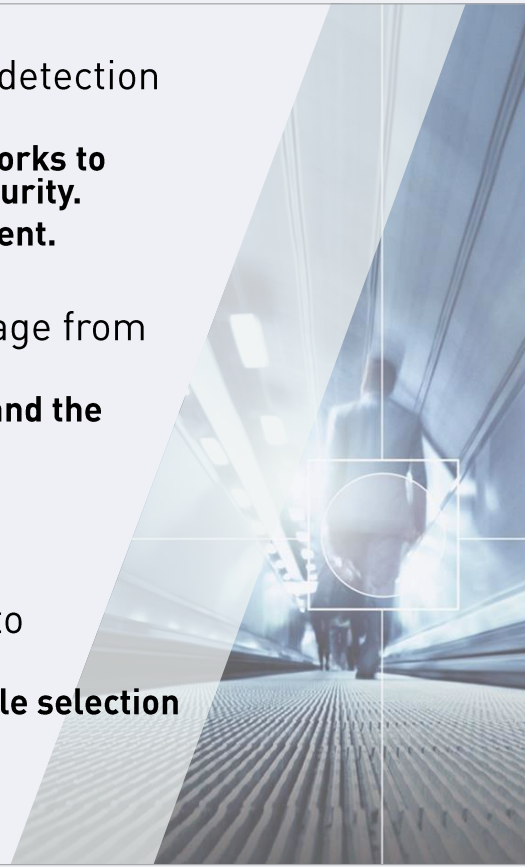
6

Problem Statements

- Which SIEM use cases do I need to implement to achieve a good threat detection maturity? - how do I measure the threat detection maturity?
  - **Use the SIEM UC Selection methodology supported by standards and frameworks to evaluate your required SIEM use cases to realize a good threat detection maturity.**
  - **Ability to measure your detection maturity by required UC and their deployment.**

- Which log sources are important to establish a reliable detection coverage from an early stage? – how do I measure the threat detection coverage?
  - **Consider endpoint logs, or better EDR, for real-time pre-analysis of attacks and the capability for response activities.**
  - **Additional log feeds for alert enrichment and deep analysis.**
  - **Direct relationship between the EDR deployment and the detection coverage.**

- How can existing cybersecurity standards and frameworks be mapped to threats and detection capabilities?
  - **Use the SIEM UC Selection methodology to have a comprehensible and reliable selection process for identification of the adequate SIEM UC to fulfil the standards and frameworks.**



Key take aways

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

- Threat Detection Roadmap capabilities
- Comprehensible and defined SIEM UC selection process
- Relationship between standards/frameworks and the SIEM UC for the security detection maturity
- Measurable and reportable added values of a SOC by the UC required based on standards/frameworks
- Endpoint as the most powerful log feed for anomaly detection

Questions & Answers

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

? & !


ISPIN AG ZURICH
swiss made security.®
Member of CymbiQ Group
Together. Secure.
Thank you very much for your attention!
persistent security in a changing world.