SIEM Betrieb im SOC

Strategien zur Erkennung
und
Reaktion auf Cyber-Sicherheitsvorfälle,

Alexander Koderman, verinice.XP 2019

87% aller Cyber-Angriffe finden innerhalb weniger Minuten statt.

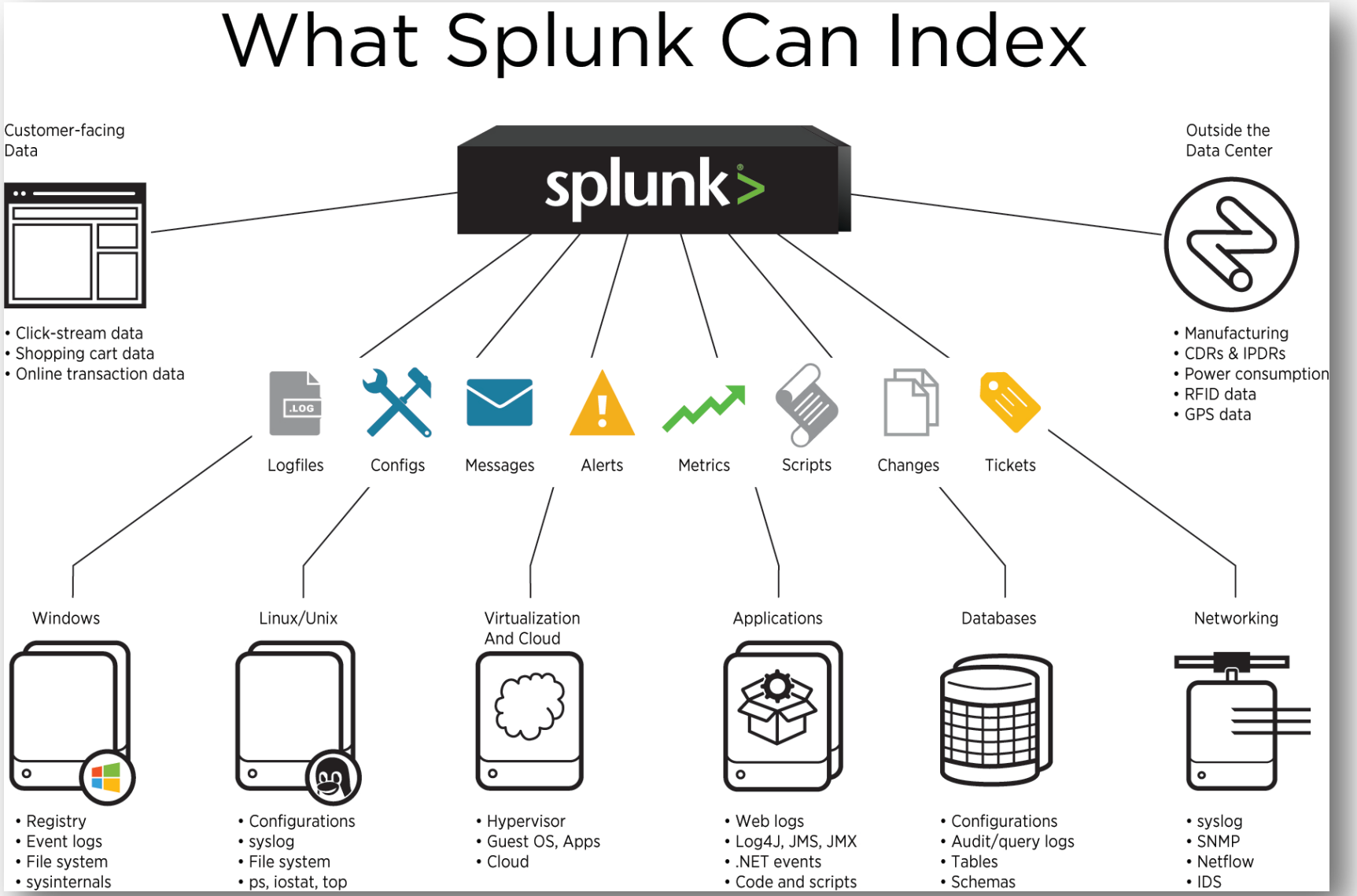
(Quelle: Verizon Data Breach Investigations Report 2018)

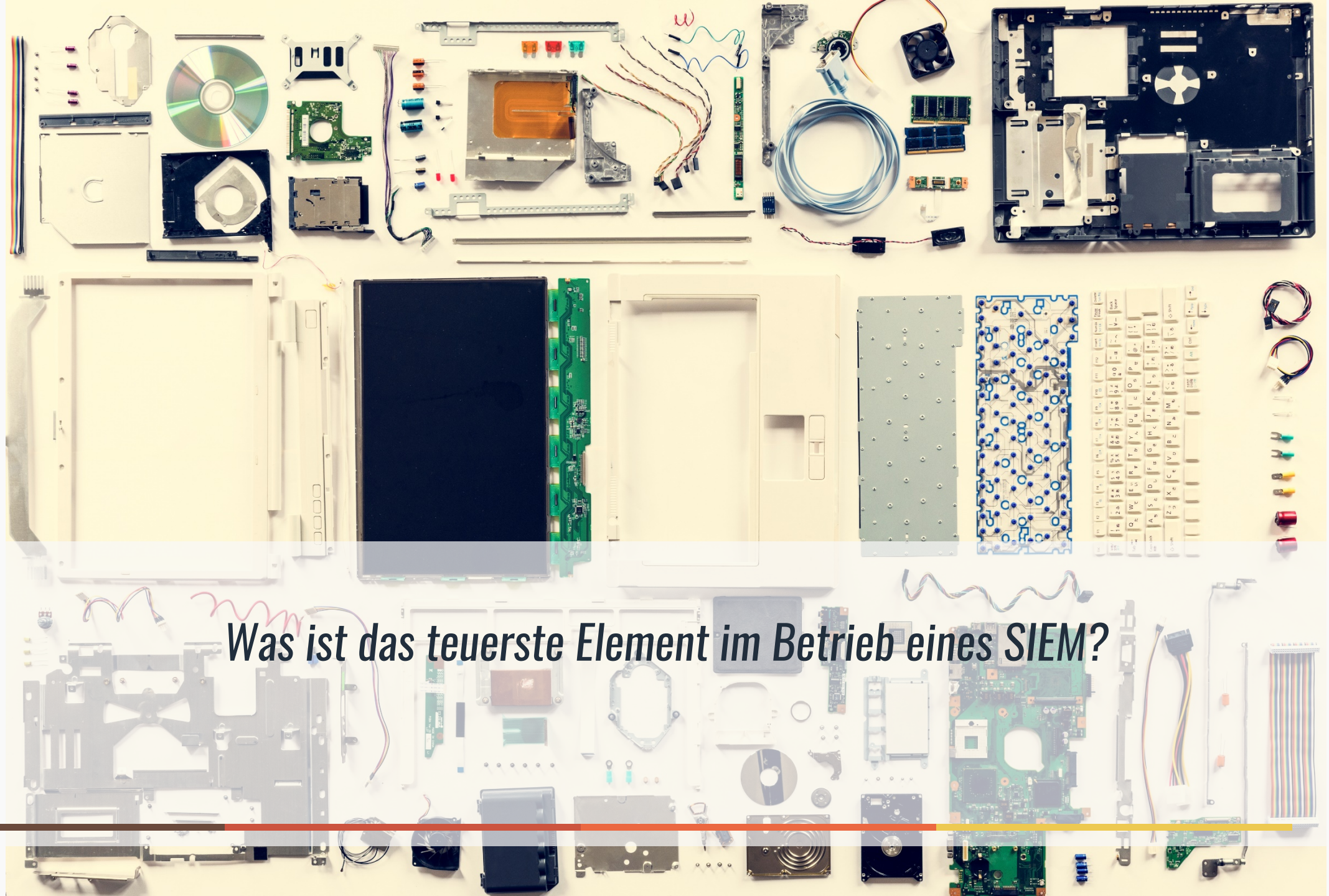
3% aller Cyber-Angriffe werden innerhalb weniger Minuten erkannt.

68% aller Cyber-Angriffe werden erst nach einigen Monaten aufgedeckt.

SIEM: Security Information and Event Monitoring

(Quelle: Splunk Inc.)

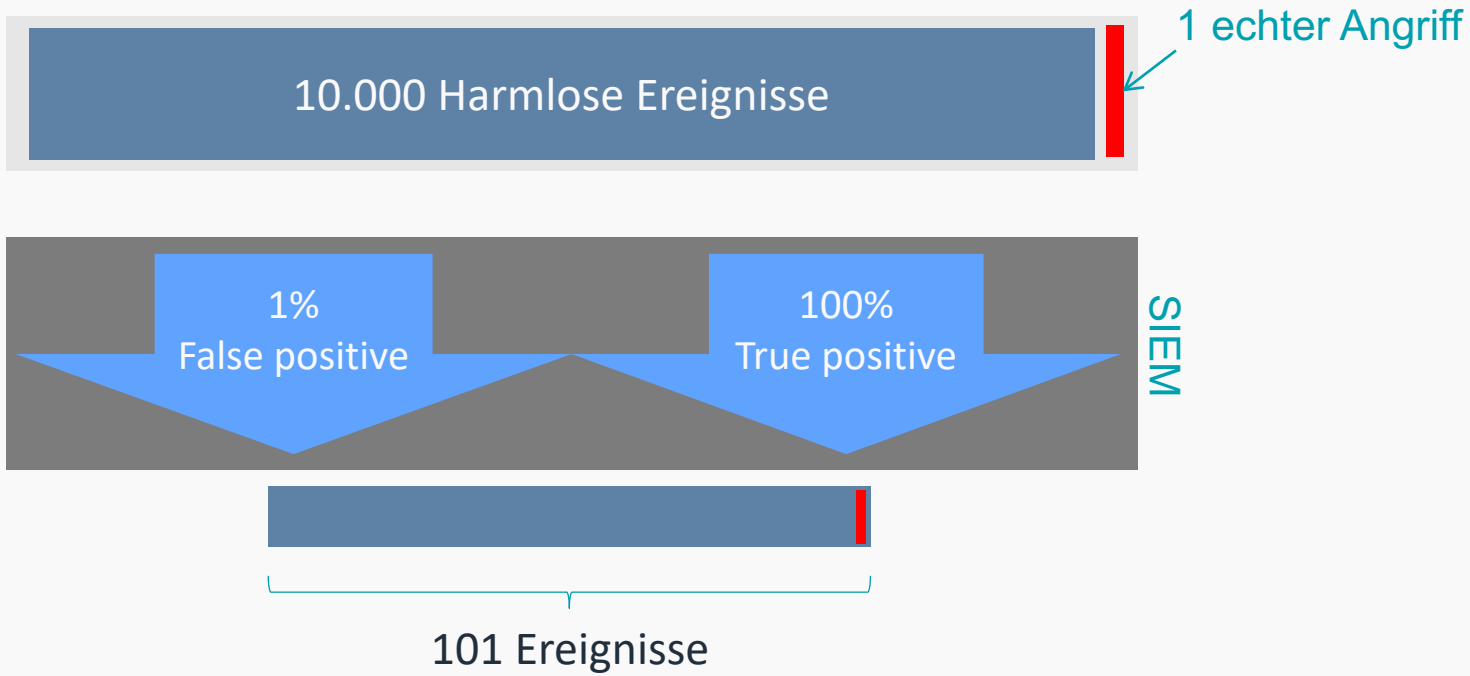




Was ist das teuerste Element im Betrieb eines SIEM?

Let's talk about Basisratenfehler

(Base Rate Fallacy)



SIEM Betrieb im SOC

Inhalt

SOC, CERT, CSIRT, SIEM und co.

Ein paar Begriffsdefinitionen.

Datenquellen

Klassifikation von Datenquellen und Sensoren.

Vantage Risk und andere Fallstrippen.

Misserfolgsfaktoren

Wie kann ich sicher stellen, dass mein SIEM Projekt garantiert auf spektakuläre Weise fehlschlägt?

Use Cases

Auswertungsregeln, Reporting und Alerts.

SIEM Prozesse

Notwendige Aufbau- und Ablauforganisation für den SIEM-Betrieb

Kosten

Was ist für Ramp-Up und Betrieb zu berücksichtigen?

SOC, CERT, CSIRT, SIEM und Co.

Eine paar Begriffsdefinitionen

SIEM

Security Information and Event Monitoring: Aggregation, Korrelation von Logfiles und anderen Datenquellen. Auswertung und Benachrichtigung.

Log Monitoring

Sammlung und Auswertung, Benachrichtigung

Log Management

Konfiguration, Homogenität, Sammlung und Speicherung

PAM

Privileged Access Management: Überwachung und Freigabe administrativer / privilegierter Zugriffe

SOC, CERT, CSIRT, SIEM und Co.

Eine paar Begriffsdefinitionen

SOC (Bedeutung 1)

Security Operating Center:
Einheit in einer großen Organisation, welche die Funktionen anderer Bereiche spiegelt, um schnell auf Sicherheitsereignisse reagieren zu können.

SOC (Bedeutung 2)

Security Operating Center:
Einheit in einer Organisation, welche sicherheitskritische Infrastruktur überwacht und auf Sicherheitsereignisse angemessen reagieren kann.

CERT

Computer emergency response team:
Einheit in einer Organisation zur Sicherheitsvorfallbehandlung und –vorbeugung.
Trademark der Carnegie Mellon University.

CSIRT

Computer Security Incident Response Team:
Markenrechtlich nicht geschützter Oberbegriff für CERTs.

Klassifikation von Datenquellen

(Michael Collins: Network Security Through Data Analysis, 2nd Edition)

01

Vantage

Platzierung im Netzwerk. Unterschiedliche Sichten auf dasselbe Ereignis.

02

Domain

Die Informationsebene des Sensors / der Datenquelle.

03

Action

Wie liefert / manipuliert der Sensor ein Ereignis?

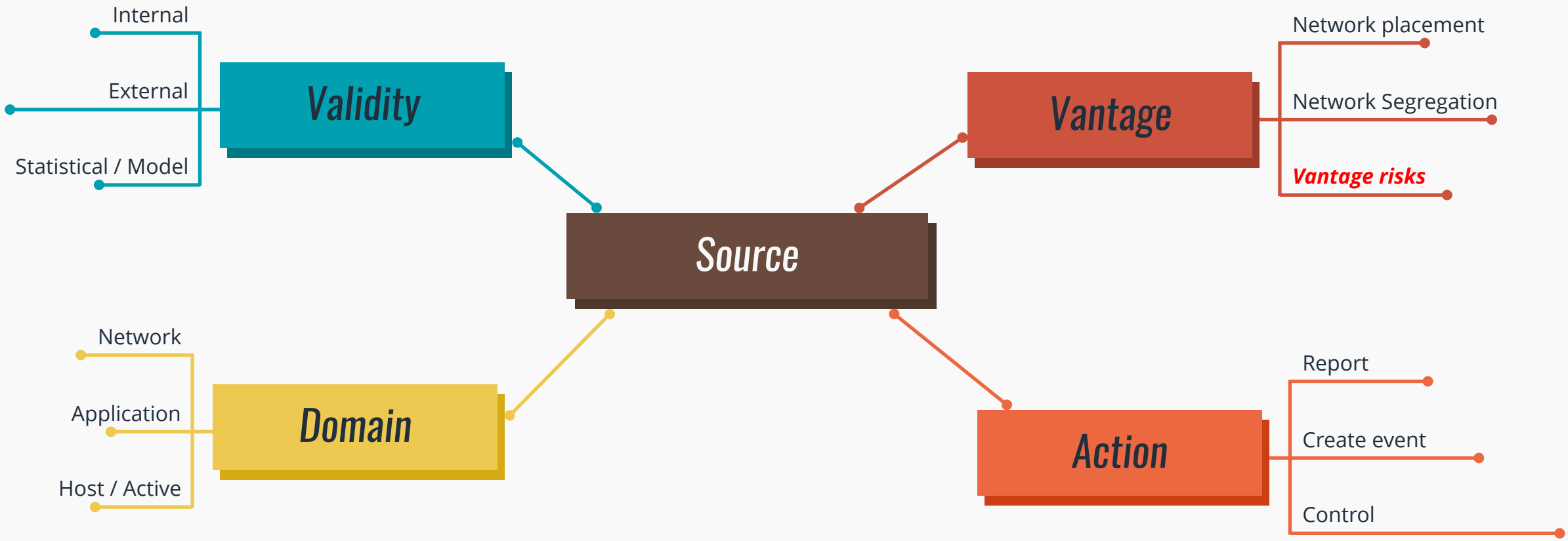
04

Validity

Ergebnis der vorherigen Attribute: Gültigkeit der Bewertung des Ereignisses.

Klassifikation von Datenquellen

(Michael Collins: Network Security Through Data Analysis, 2nd Edition)



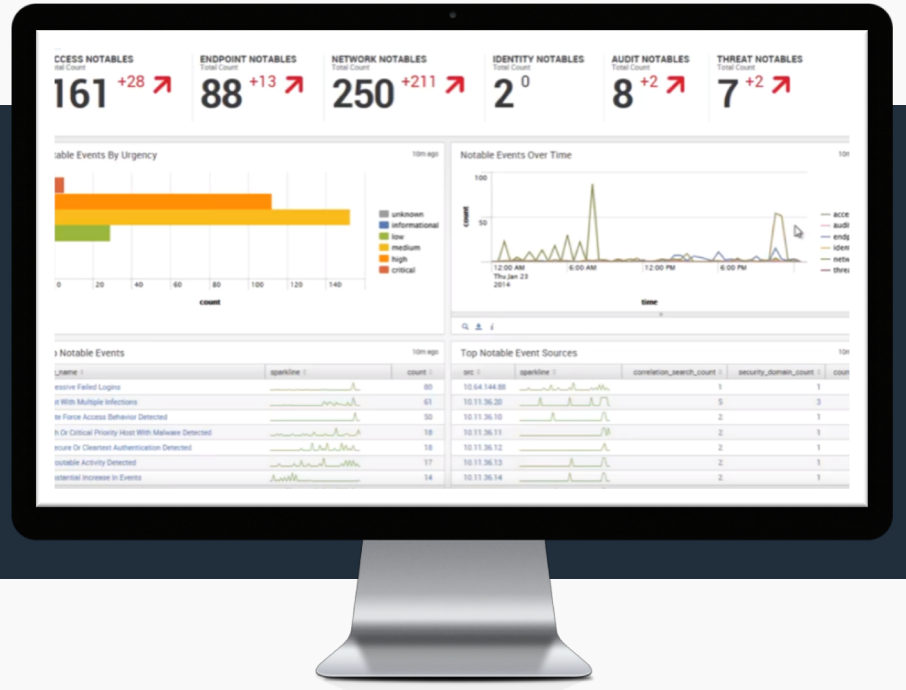
Vantage Risks: Identity, Causality, Aggregation, Consistency, Encryption

Misserfolgsfaktoren

Wie garantiere ich das Scheitern meines SIEM-Projekts?

- Nur Application-Logs (nur OS-Logs / nur DB-Logs / ...)
- Unterschiedliche Timestamps
- Unterschiedliches Logformat
- Weniger ist mehr !
- Oder: LOG_LEVEL_DEBUG_VERBOSITY_VERY_VERBOSE

Log Management



Misserfolgsfaktoren

Wie garantiere ich das Scheitern meines SIEM-Projekts?

- AD-Updates / Logon / Logoff nicht auswerten!
- Kein Session Manager, kein Session Monitor.
- Sende 30.000 “sudo” Aufrufe pro Tag zur Verifikation an den Prozesseigentümer!

Privileged Access Management

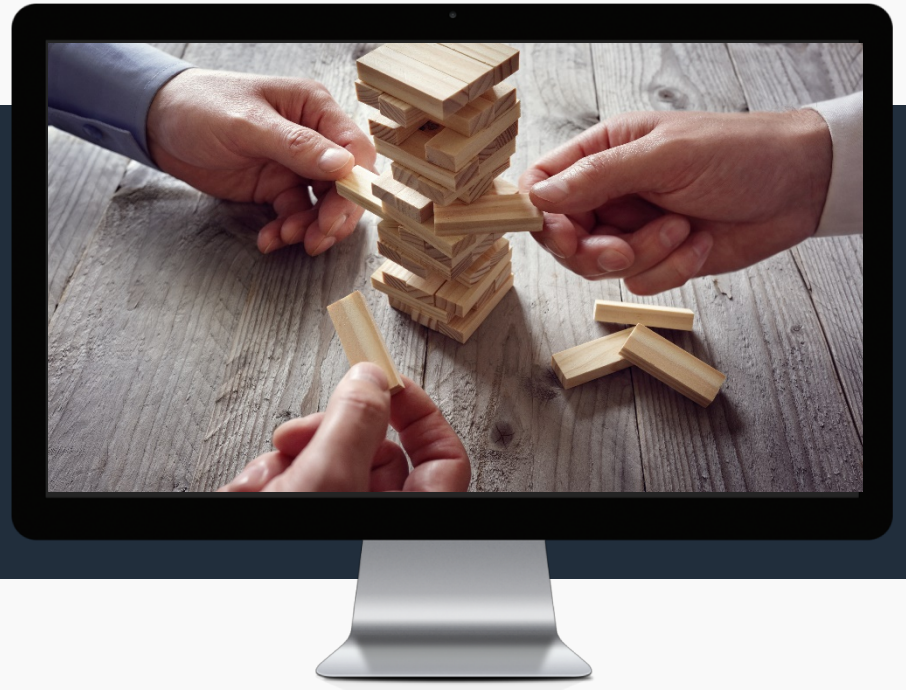
Source: https://security-architect.com/privileged-account-management-pam-is-very-important-but-deploying-it-stinks/

Misserfolgsfaktoren

Wie garantiere ich das Scheitern meines SIEM-Projekts?

- Betrieb einer Anwendung auf möglichst viele Dienstleister verteilen!
- Uneinheitliche Leistungsebene: OS, DB, Applikation, Netz…
- Keine Inventarisierung, keine Netzpläne pflegen.
- Multi-Cloud!
    - (Ohne Governance, ohne Referenzarchitektur, ohne ISO 27017.)

Outsourcing



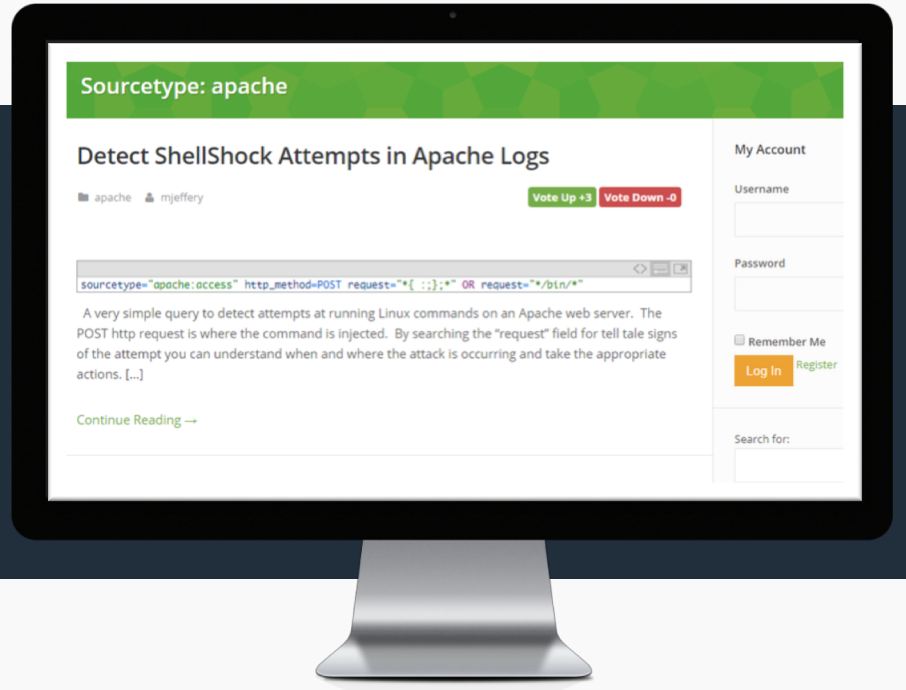
Source: https://security-architect.com/privileged-account-management-pam-is-very-important-but-deploying-it-stinks/

Misserfolgsfaktoren

Wie garantiere ich das Scheitern meines SIEM-Projekts?

- Das Tool bringt ja Auswertungsregeln mit.
- Davon ausgehen, dass die auf die vorhandenen Datenquellen passen.
- Kein Konzept für die Use Cases erstellen.
- Die Business Owner müssen wir damit nicht belasten.
- Versionskontrolle auf den Abfragen ist nicht nötig.

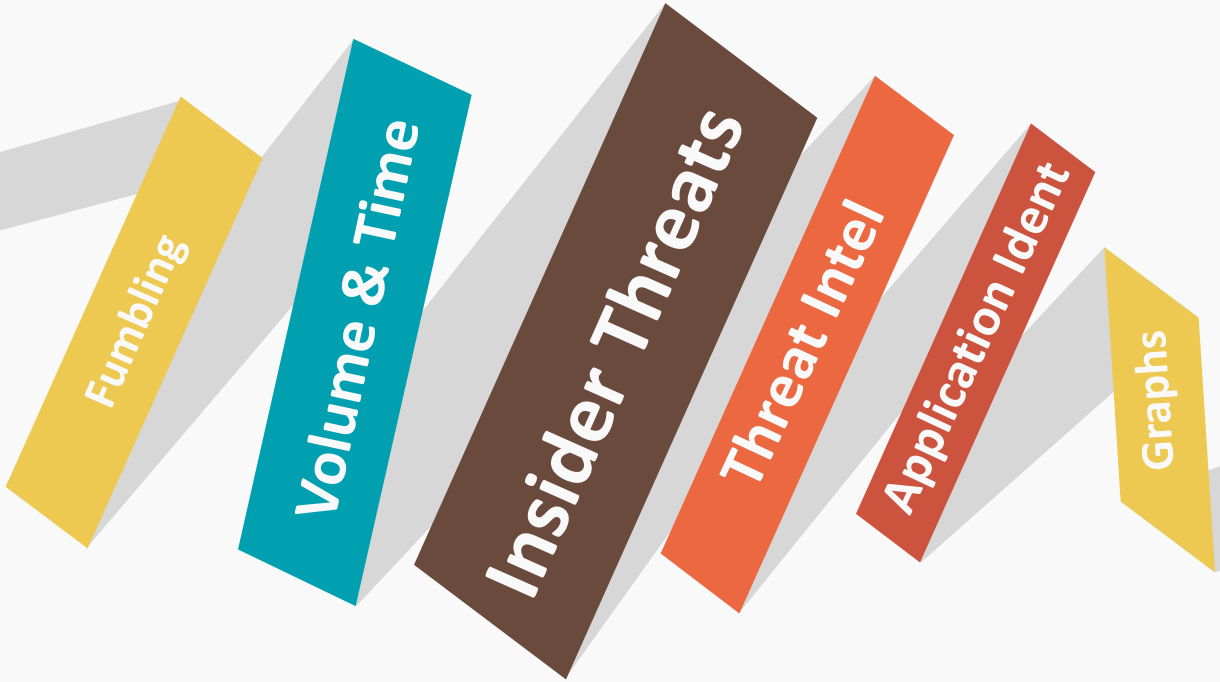
Use Cases



Source: https://security-architect.com/privileged-account-management-pam-is-very-important-but-deploying-it-stinks/

Use Cases

Auswertungsregeln

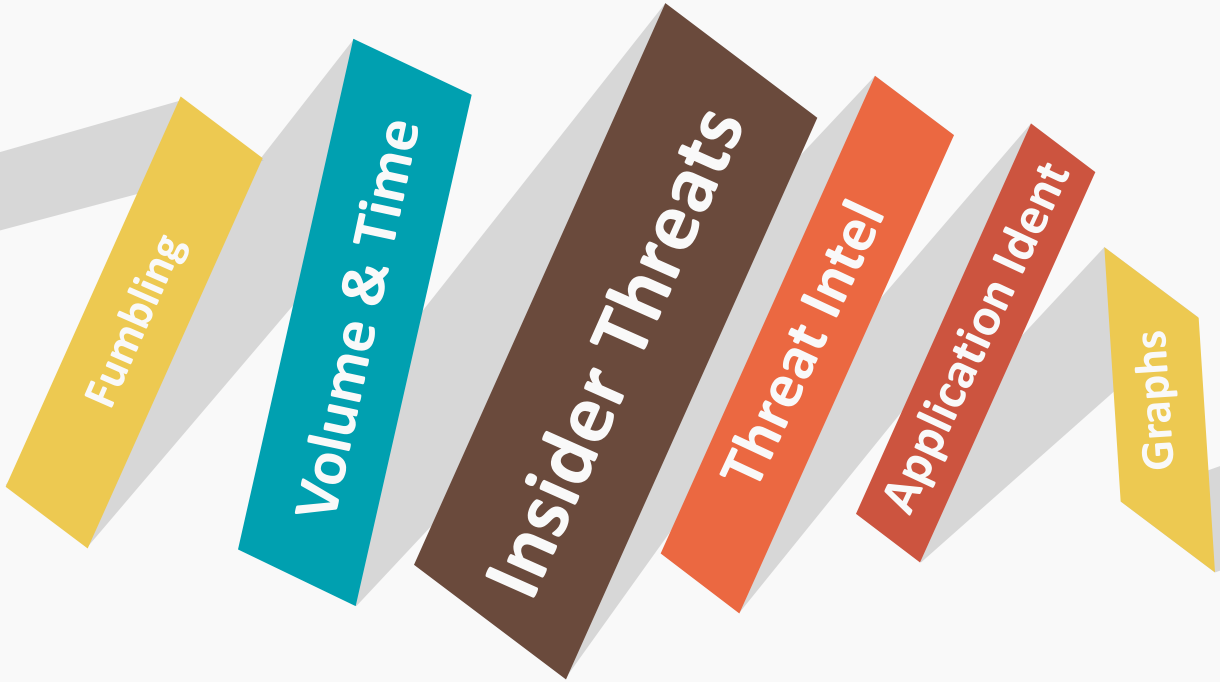


Fumbling

- Misconfiguration, Automation, Scanning
- Lookup Failures
- IP Fumbling (Dark Space / Spread)
- TCP Fumbling: Failed Sessions
- Also ICMP, HTTP, SMTP, DNS

Use Cases

Auswertungsregeln

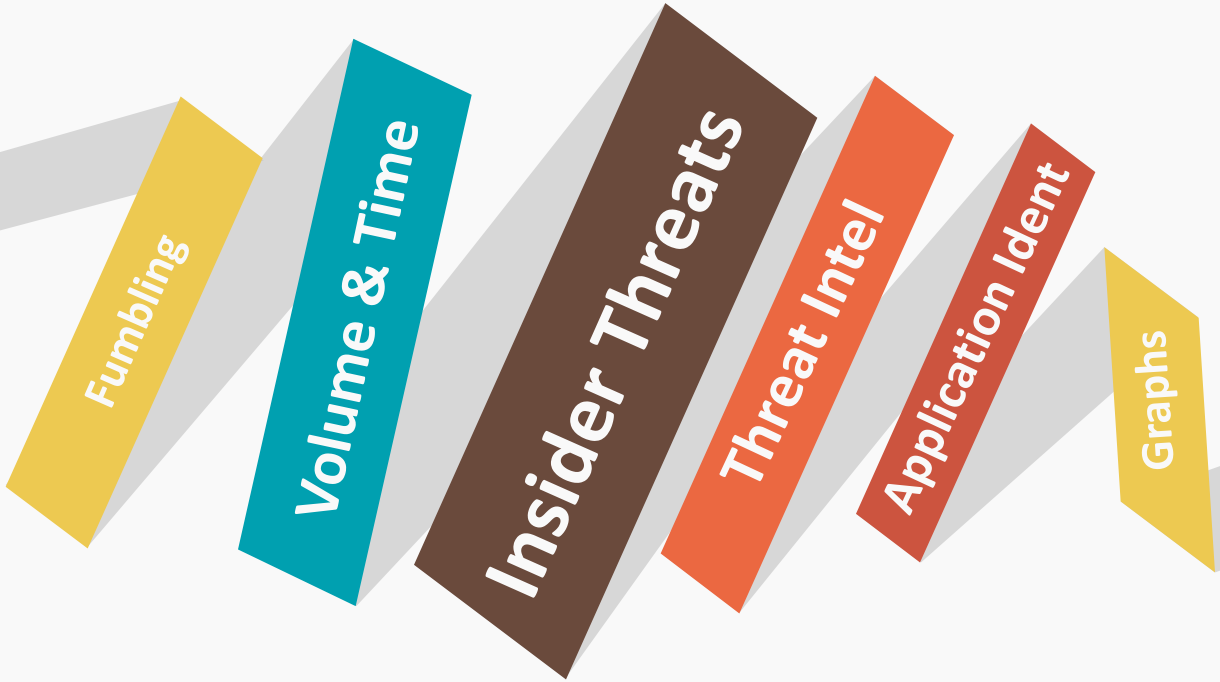


Volume & Time

- Beaconing
- File Extraction, File Transfer, Raiding
- DDoS, Flash Crowd, Cable Cuts

Use Cases

Auswertungsregeln



Threat Intelligence

- Network repudiation information
  - IoCs
  - TTPs

Use Cases

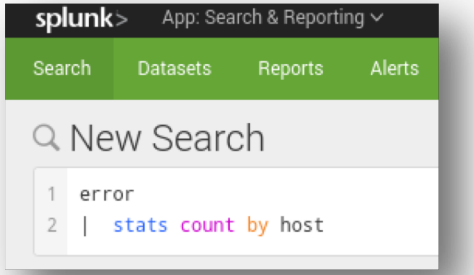
Abbildung auf Compliance-Vorgaben

		HIPAA -> 164.312: 164.312(b) GLBA -> 314.4: 314.4(b)(2), 314.4(b)(3) GLBA -> 6801: 6801(b)(2), 6801(b)(3) SANS -> CIS: CSC 12, CSC 14, CSC 16 NIST Special Publication 800-53 Rev 4: AC-1, AC-2	
10	Benutzerkonto ändern	ISO/IEC 27001:2013: A.9.2.1 COBIT 5: DSS05.04, DSS06.03 ISA 62443-2-1:2009: 4.3.3.5.1 ISA 62443-3-3:2013: SR 1.1, SR 1.2, SR 1.3, SR 1.5, SR 1.7, SR 1.8, SR 1.9 PCI DSS 3.1: 08.01.2003 SOX-> ITGC-> Continuous Control Monitoring (Automated) + Logging and Monitoring + Sensitive Access Report HIPAA -> 164.308: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C) HIPAA -> 164.312: 164.312(e)(1) GLBA -> 314.4: 314.4(b)(2), 314.4(b)(3) GLBA -> 6801: 6801(b)(1), 6801(b)(2), 6801(b)(3) SANS -> CIS: CSC 16 NIST Special Publication 800-53 Rev 4: AC-1, AC-2	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
11 / 12	Benutzerkonto sperren	NIST Special Publication 800-53 Rev 4: AC-1, AC-2	AC-1, AC-2, IA-1, IA-2,
13	Passworte eines Benutzers durch Administrator verändern	ISO/IEC 27001:2013: A.9.2.1 COBIT 5: DSS05.04, DSS06.03 ISA 62443-2-1:2009: 4.3.3.5.1 ISA 62443-3-3:2013: SR 1.1, SR 1.2, SR 1.3, SR 1.5, SR 1.7, SR 1.8, SR 1.9 PCI DSS 3.1: 08.02.2002, 10.02.2002, 10.02.2005 SOX-> ITGC-> Continuous Control Monitoring (Automated) + Logging and Monitoring HIPAA -> 164.308: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C) GLBA -> 314.4: 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C) GLBA -> 6801: 6801(b)(1), 6801(b)(2), 6801(b)(3) SANS -> CIS: CSC 16 NIST Special Publication 800-53 Rev 4: AC-1, AC-2, AU-2, IA Family	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

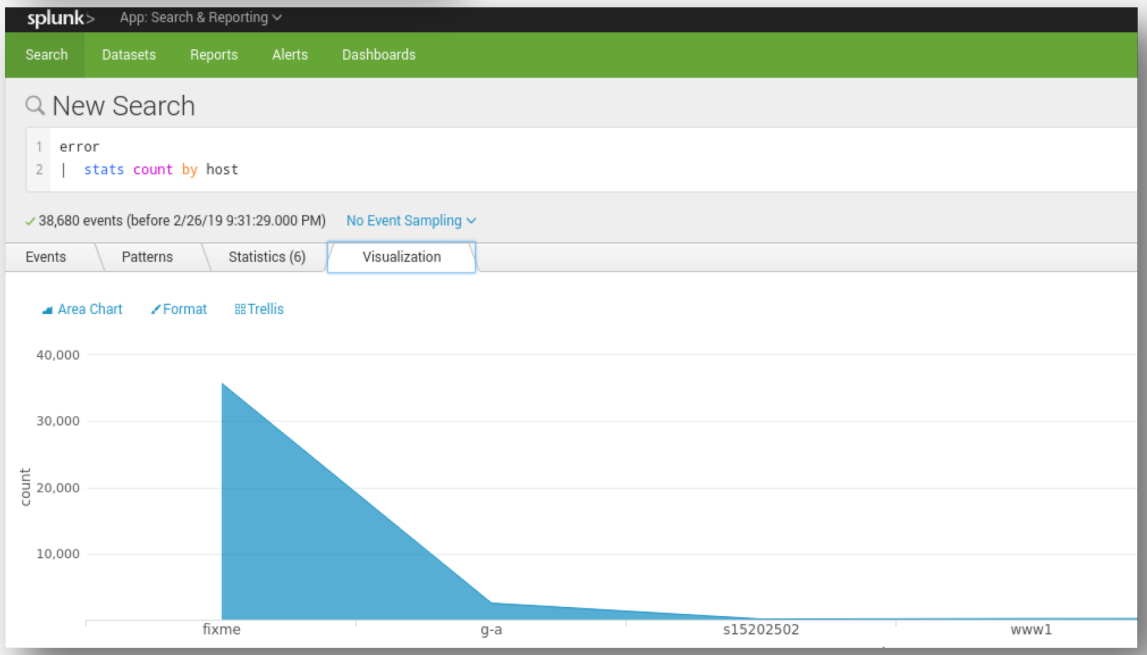
Quelle: Shoogee GmbH, http://www.shoogee.com/de/it-consulting.html#siem

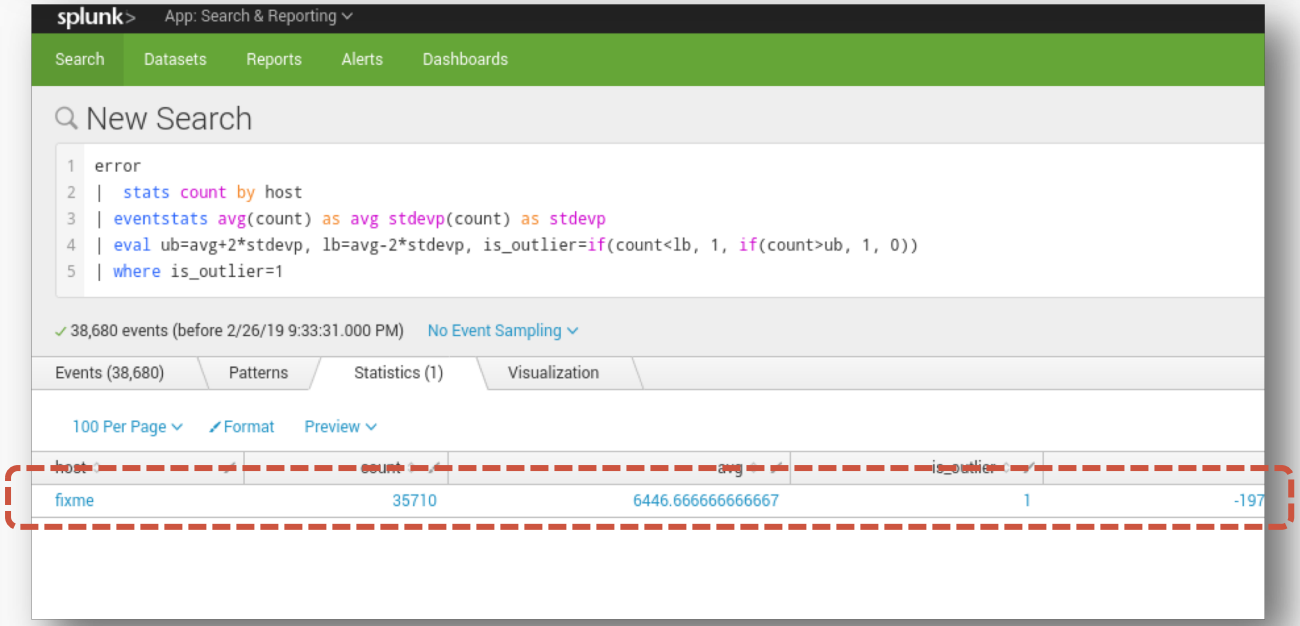
Use Cases

Monitoring Rules vs. Alerting Rules



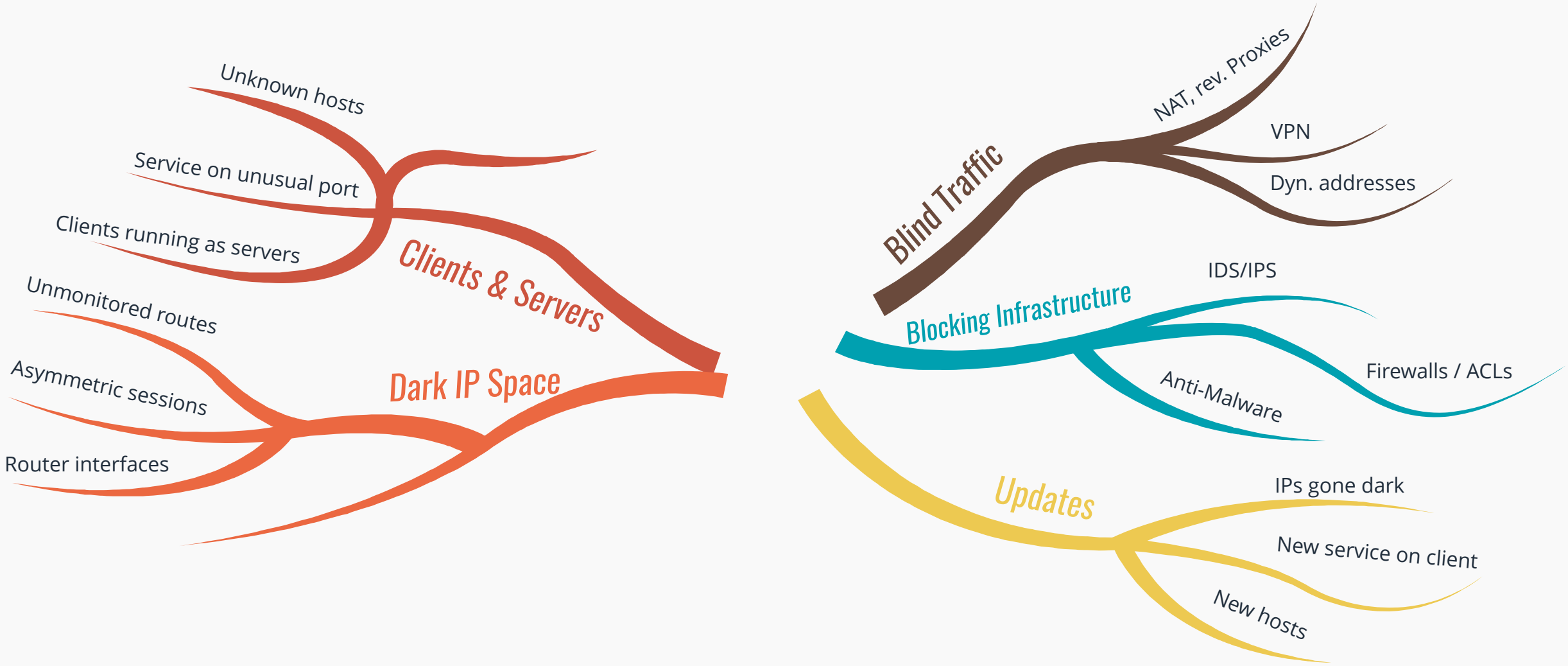

```
error
| stats count by host
| eventstats avg(count) as avg stdevp(count) as stdevp
| eval ub=avg+2*stdevp, lb=avg-2*stdevp, is_outlier=if(count<lb, 1, if(count>ub, 1, 0))
| where is_outlier=1
```





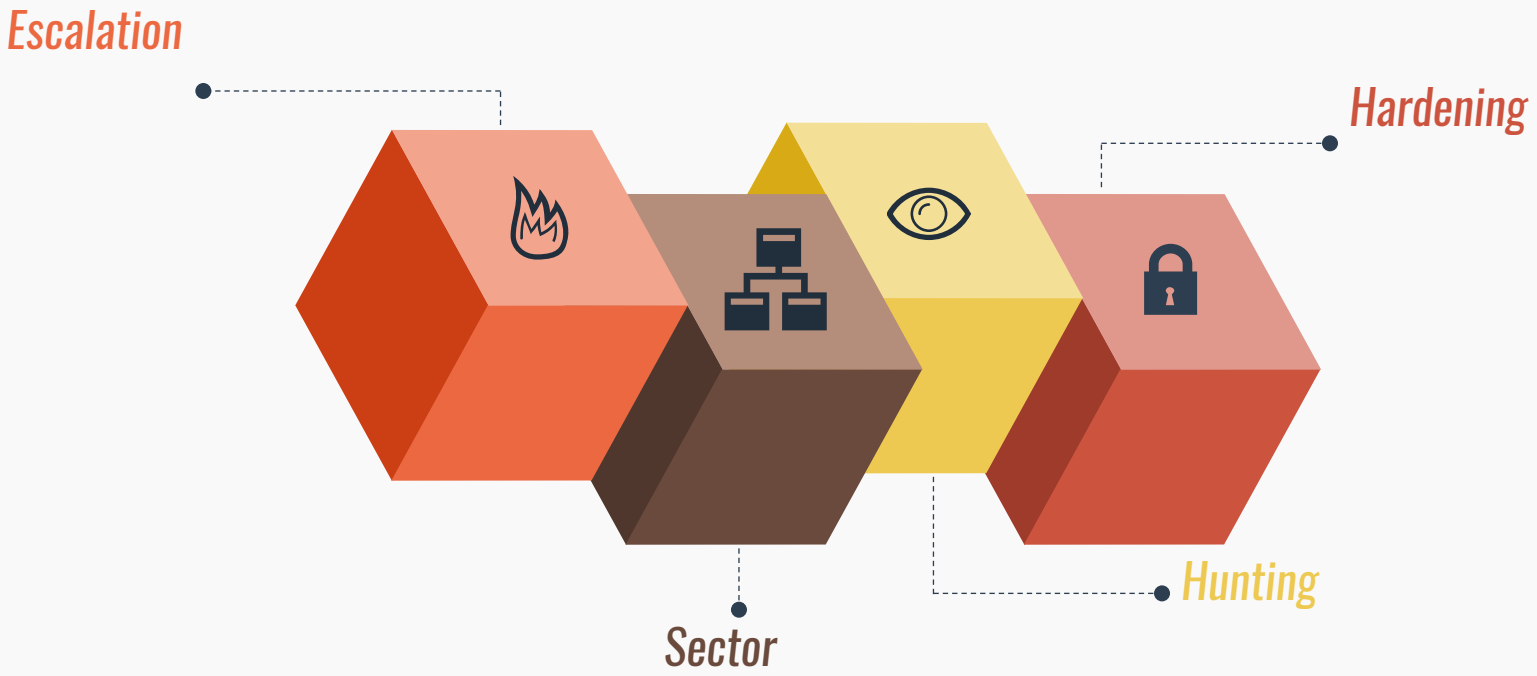
Das Anti-Inventory

Die dunkle Materie des IT-Betriebs



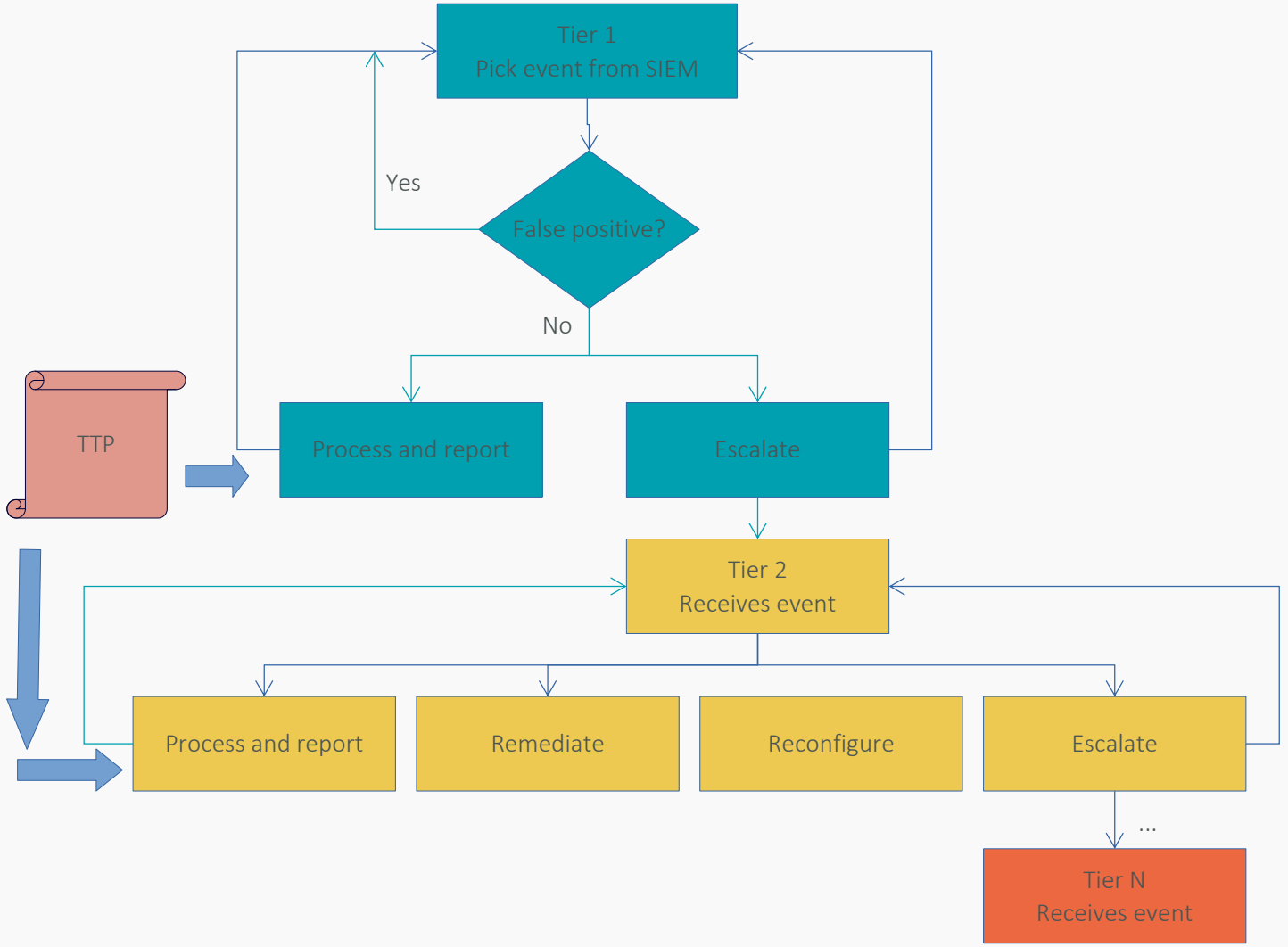
SIEM Prozesse

Tätigkeiten für das SOC-Team



SIEM Prozesse

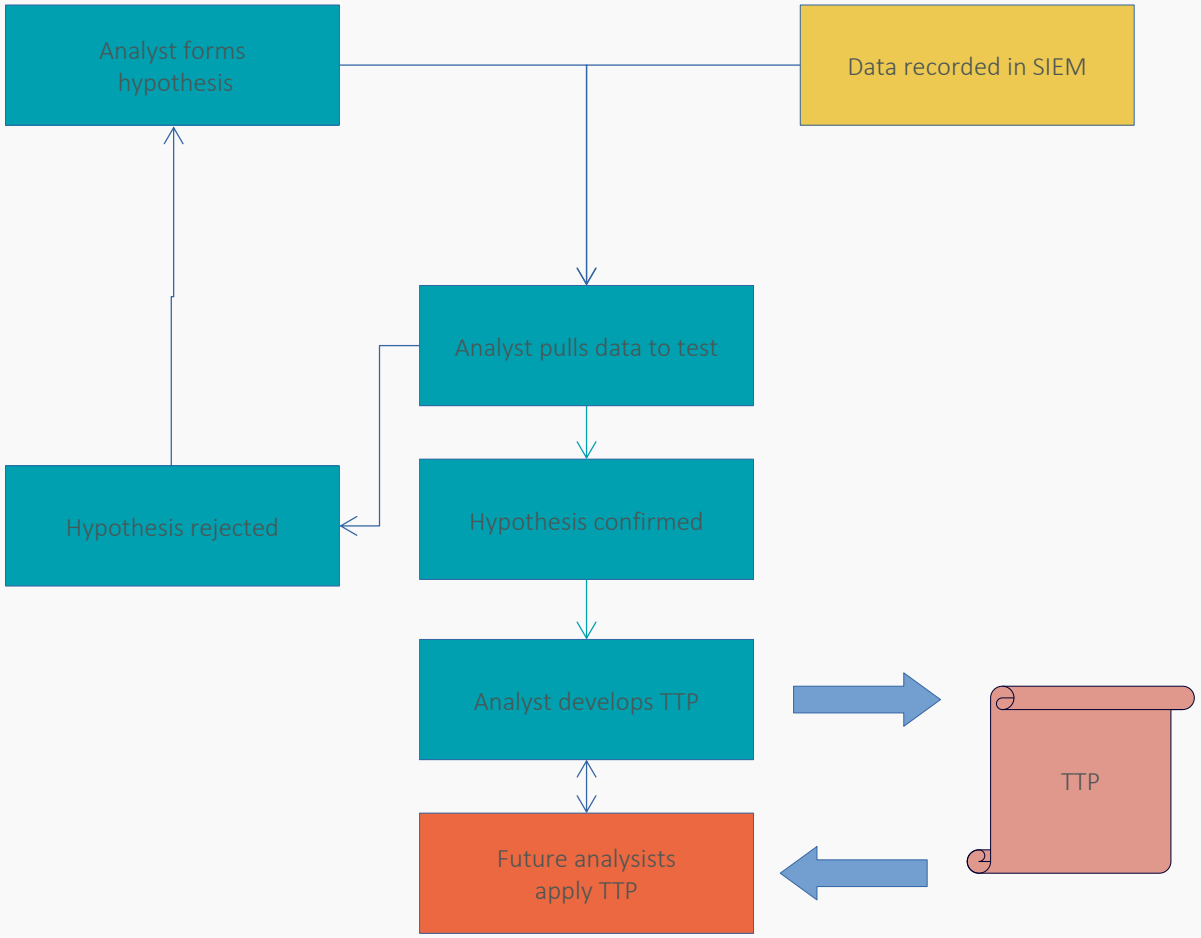
Escalation (vergl. NIST 800-61)



Quelle: Michael Collins: Network Security Through Data Analysis, 2nd Edition

SIEM Prozesse

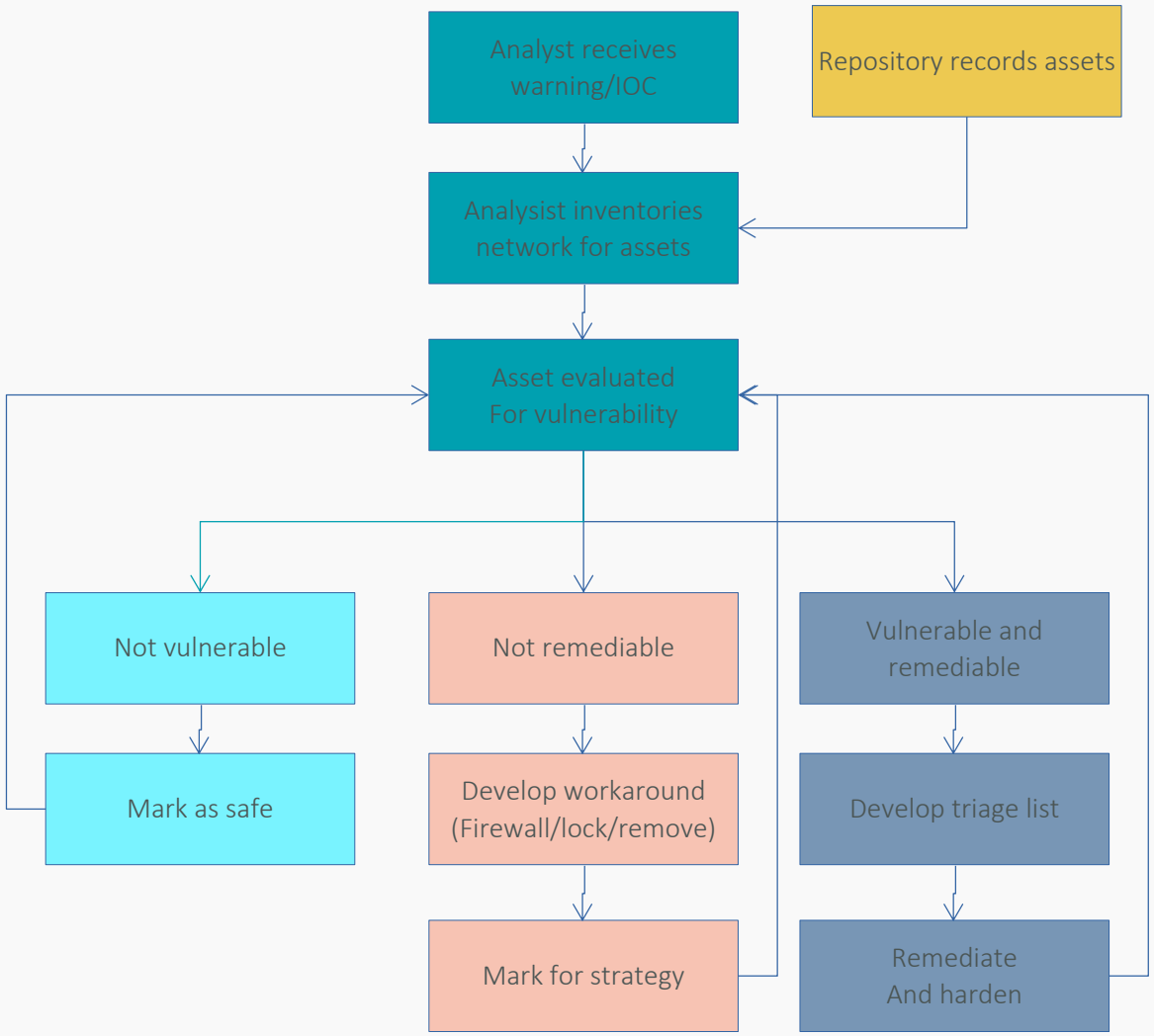
Hunting



Quelle: Michael Collins: Network Security Through Data Analysis, 2nd Edition

SIEM Prozesse

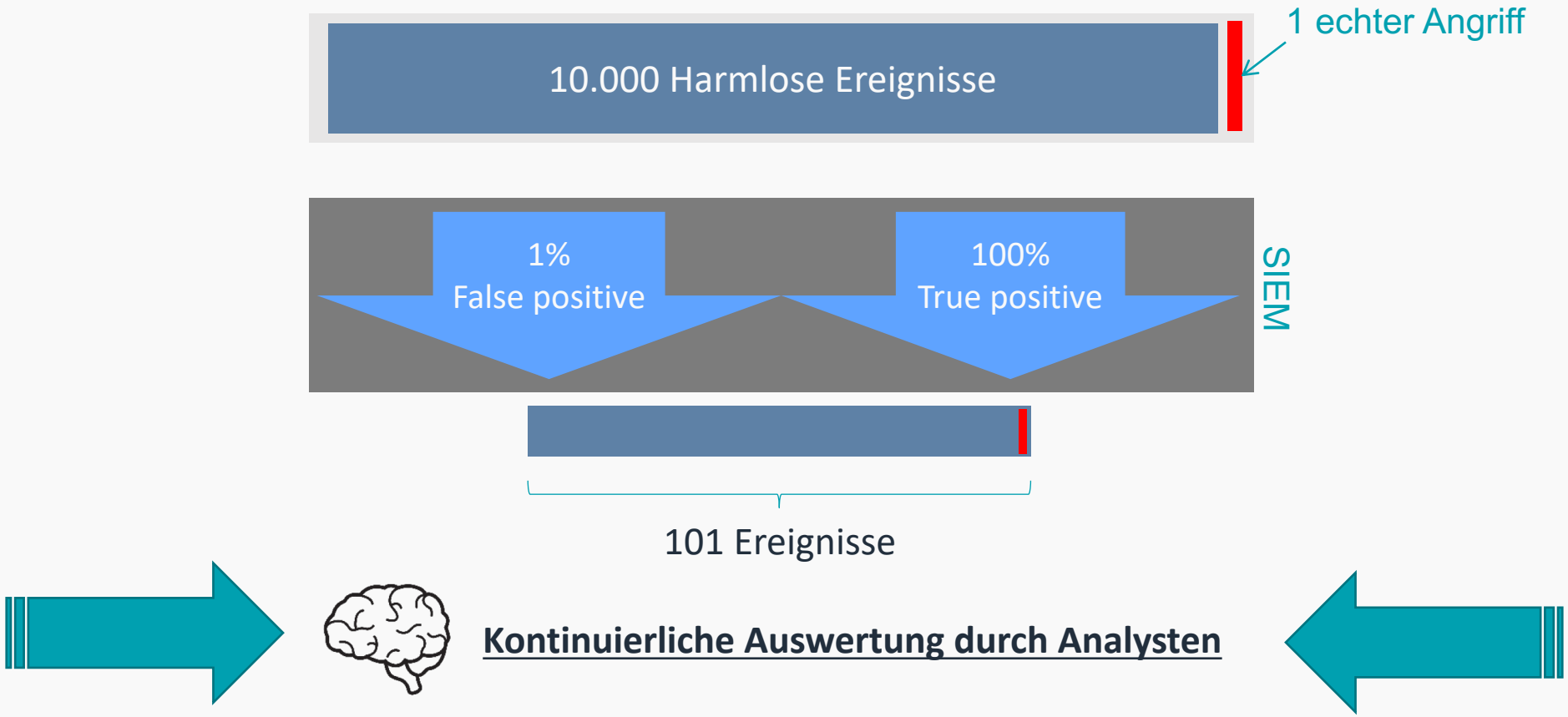
Hardening



Quelle: Michael Collins: Network Security Through Data Analysis, 2nd Edition

Zurück zum Basisratenfehler

Und zur Auflösung der Frage



SIEM Kosten

Für Ramp-Up Projekt und Betrieb

Hardware

SIEM Server, Appliance oder Cloud Service.

Storage: z.B. 0,2-30GB täglich pro Anwendung.

Retention 6 Monate: 36-5400GB,

Throughput: EPS: 3 (Windows Server) – 30 (Netflow/IPFIX)

Software

SIEM-Lizenz und jährliche Maintenance.

Professional Services

PoC, Sizing, Installation, Konfiguration, Erhebung und Umsetzung von Use Cases, Änderungen an Log-Konfiguration ...

Feeds

TTPs, IOAs, IOCs, vulnerabilities, network repudiation, cloud audit trails...

Personal

SIEM Analysten:

Junior Lvl: 10-15 Events/Stunde (Escalation)

Senior Lvl: 1-0,05 Events/Stunde (Hunting)

Software-Kosten

z.B. Splunk perpetual vs. annual license (Quelle: Splunk, März 2017)

Daily Index	Perpetual License	Annual Term License
Volume	(per GB)	(per GB)
1 GB/day	$4,500	$1,800
10 GB/day	$2,500	$1,000
50 GB/day	$1,900	$760
100 GB/day	$1,500	$600
>100 GB/day	Contact Sales	Contact Sales

50 GB/day License	Perpetual Cost	Perpetual Total	Term Total	Annual Term Cost
Year 1	$95,000 + $19,000 support	$114,000	$38,000	$38,000
Year 2	$19,000	$133,000	$76,000	$38,000
Year 3	$19,000	$152,000	$114,000	$38,000
Year 4	$19,000	$171,000	$152,000	$38,000
Year 5	$19,000	**$190,000**	**$190,000**	$38,000
Year 6	$19,000	$209,000	$228,000	$38,000