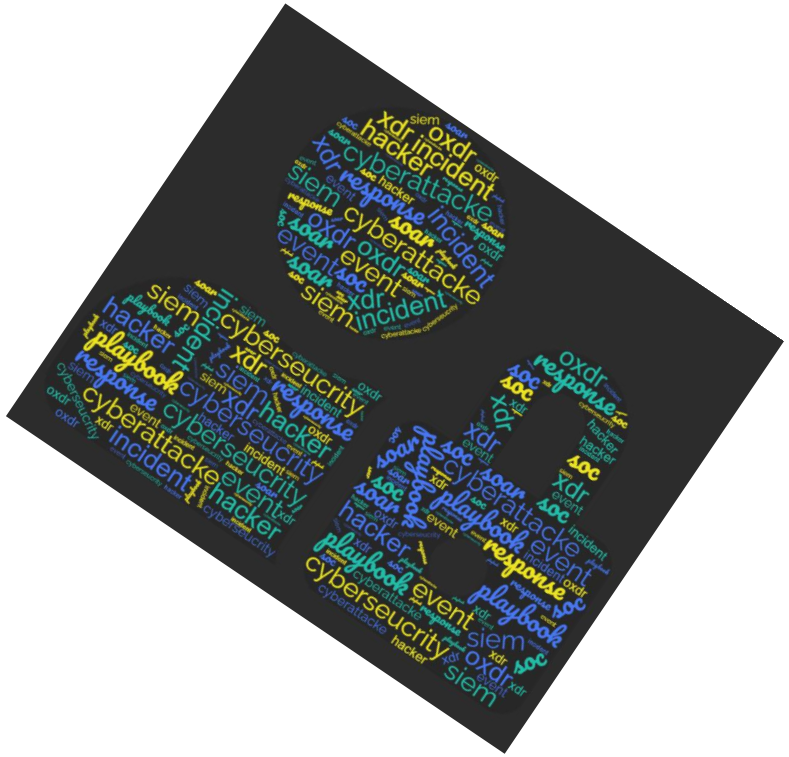
«SIEM (SOAR / EDR / XDR) & SOC»

Cyberattacken erkennen?
Security Monitoring & Response



19. SRT

hacker inside

Über UZH

- UZH:
  - ~28’000 studierende
  - 7300 Mitarbeiter (VZÄ, ~10’000 MA)
  - 150 Institute mit dezentraler IT und IT- Verantwortung
  - Zentrale Informatik für Grundservices wie Netzwerk / Datacenter / Managed Endpoint auf Wunsch / zentrales Server Hosting etc. ~200 MA
  - >220 Gebäude
  - Mehrheitlich BYOD
- Etat der UZH 1.5 Mrd CHF vgl. Jahresbericht der UZH 2022
  - 208 Mio CHF Dienstleistungs- und übrige betriebliche Erträge (Risiken)
- Persönlich
  - Sacha Schweizer Leiter IT- Sicherheitsstelle und Security Operation Center ZI / UZH , 23 Jahr im IT- Sicherheitsbereich tätig (SOC / Penetrationtesting / Schwachstellenmanagement / Netzwerksicherheit /Techn. Sicherheitsarchitektur resp. Orchestrierung IT-Sicherheitsbausteinen)
  - Informatiker Software Engineer / Certified Ethical Hacker / Dipl. Betriebswirtschafter / Dipl. Braumeister

„Angesichts der zunehmenden Angriffsoberfläche und der immer kürzeren Angriffszeiten sind Geschwindigkeit und Effizienz von grundlegender Bedeutung für den Erfolg ressourcenbeschränkter Sicherheitsteams“

Wichtig: Mit den Cybersecurity Bedrohungen mit wachsen

Agenda

- Kurzer (sehr, sehr kurzer) Abriss über Entwicklung von SIM/ SEM zu SIEM
- Entwicklung von SIEM zu XDR
- Wege zu einem Security Monitoring & Response (SIEM / XDR / Org. etc.)

Kurzer (sehr, sehr kurzer) Abriss über Entwicklung von SIM/ SEM zu SIEM

Cyber Attacken an Hochschulen 2016 / 17

Mutmasslicher Hacker verhaftet

19.02.2016 | Medienmitteilung

Ende Januar 2016 ist ein Hacker unbefugt in das IT-System der ETH Zürich eingedrungen. Durch das schnelle Eingreifen und die gute Zusammenarbeit von Staatsanwaltschaft, Polizei und ETH Zürich konnte eine verdächtige Person kurz nach Entdeckung des Eindringens verhaftet werden. Beim Verdächtigen handelt es sich um einen ETH-Studierenden.

Im Januar 2016 hat sich ein unbekannter Täter unerlaubt Zugang zum IT-System der ETH Zürich verschafft, sich so ins Netzwerk der ETH Zürich eingeloggt, über das ETH-System Software bestellt und Daten heruntergeladen. Mitarbeitende der Abteilungen Sicherheit und Informatikdienste der ETH Zürich hatten am 26. Januar 2016 unrechtmässige Manipulationen festgestellt. Daraufhin hat die ETH Zürich umgehend Anzeige gegen Unbekannt erstattet.

Quelle: https://www.ethz.ch/de/news-und-veranstaltungen/eth-news/news/2016/02/mm-mutmasslicher-hacker-verhaftet.html

Michigan State University has confirmed that on Nov. 13 2016 an unauthorized party gained access to a university server containing certain sensitive data.
The database, which contained about 400,000 records, included names, social security numbers and MSU identification numbers of some current and former students and employees. It did not contain passwords or financial, academic, contact or health information.

In addition, MSU is continuing to work with national experts to improve overall campus security. IT officials also are accelerating implementation of MSU's existing plan for increased security.
(ca. 3 Mio USD)

Quelle: http://msutoday.msu.edu/news/2016/msu-data-breach-exposed-records/

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Education & Family

Top university under 'ransomware' cyber-attack

By Sean Coughlan
Education correspondent

15 June 2017 | Education & Family | Share

UK universities targeted by cyber-thieves

5 September 2017 | Technology | Share

Attackers went after work on improving batteries and alternative fuels

British universities are being hit by hundreds of successful cyber-attacks every year, reports the Times.

http://www.bbc.com/news/technology-41160385

University pays $20,000 to ransomware hackers

8 June 2016 | Technology | Share

The University of Calgary transferred 20,000 Canadian dollars-worth of bitcoins ($15,780; £10,840) after it was unable to unwind damage caused by a type of attack known as ransomware. The malware caused emails and other files to become encrypted.

Quelle: http://www.bbc.com/news/technology-36478650

Hat die NSA Server der Uni Genf für Cyberangriffe missbraucht?

Der US-Geheimdienst habe weltweit Server diverser Universitäten für Cyberangriffe missbraucht. Auch die Uni Genf könnte betroffen sein.

Die Hackergruppe namens Shadow Brokers hat Daten veröffentlicht, die zeigen sollen, dass der US-Geheimdienst NSA weltweite Hunderte Server diverser Universitäten für Cyberangriffe missbraucht hat. Gemäss «Watson» sollen darunter auch drei Server der Universität Genf sein.

Quelle: http://www.tagesanzeiger.ch/schweiz/standard/Hat-die-NSA-Server-der-Uni-Genf-fuer-Cyberangriffe-missbraucht/story/25272585

Universities face an age of cyber crime - University World News
www.universityworldnews.com/article.php?story... ▾ Diese Seite übersetzen
22.09.2017 - "Currently, **cyber attacks** on African **universities** are not regarded as serious ... According to the **Africa** Cyber Security Report 2016, African ...

RiffReporter

Cybersicherheit an Universitäten und Hochschulen ist miserabel

Wir haben Hochschulen von außen gehackt: Die IT-Sicherheit ist miserabel. Sogar vergangene Cyberangriffe von kriminellen Hackern wurden...

10.02.2023

Forschung & Lehre

Cyberkriminalität: HAW Hamburg von Hackern erpresst

Die Hackergruppe "Vice Society" hat sich zur Cyberattacke auf die Hochschule für Angewandte Wissenschaften (HAW) in Hamburg bekannt.

16.01.2023

Blick

Russische Hacker sollen Selenski-Rede an Universität Z gestört haben

30.09.2022

Hinter den massiven technischen Problemen bei der Rede von Wolodimir Selensk der Uni Zürich sollen Hacker stecken.

Tagesschau

Hamburger Hochschule wird von Hackern erpresst | tagesschau.de

Die Hackergruppe "Vice Society" hat sich zur Cyberattacke auf die HAW Hamburg bekannt. Nach Informationen des ARD-Politikmagazins Kontraste...

13.01.2023

Heise

yber-Angriff: IT der TU Freiberg weitreichend lahmgelegt

n Cyber-Angriff auf die IT der TU Freiberg in Sachsen führt zu weitreichenden nschränkungen. Zum Wochenende hat die Uni die...

.01.2023

Kurier

Hacker versuchten Angriff auf die IT der Uni Innsbruck

Unbekannte Täter haben am Wochenende einen Angriff auf die IT-Infrastruktur der Universität Innsbruck versucht.

16.01.2023

Hacker versuchten Cyber-Attacke auf Uni Graz

Der Angriff wurde am Freitag bei einem Routine-Check entdeckt. Es dürften keine Daten gestohlen worden sein.

06.02.2023

CSO Online

Hackerangriff legt Uni Duisburg-Essen lahm

vare-Attacke wurde die IT-Infrastruktur der Uni Duisburg-Essen ie Täter drohen jetzt damit,...

Aachener Zeitung

Cyberangriffe: Hacker attackieren täglich Unis und Krankenhäuser

Die Angriffe auf deutsche Universitäten aus dem Internet nehmen zu, auch die RWTH Aachen und deren Klinikum sind betroffen.

18.02.2023

SRF

Professionelle Hacker am Werk - Grosser Cyberangriff auf Uni Zürich: Polizei ermittelt

Kriminelle versuchen, in die Systeme der Universität zu gelangen. Solche Angriffe auf Hochschulen häufen sich.

03.02.2023

SRF

Internetkriminalität - Uni einer Cyberattacke

Der nächste Angriff auf Neuenburg Visier von Hackerinnen und Hacke

19.10.2022

MOPO

„Absolute Krise“: Hamburger Hochschule von Hackern attackiert

Das Jahr 2022 endete für die Hochschule für Angewandte Wissenschaften (HAW) mit einem Knall: Hacker griffen die IT-Systeme an,...

13.01.2023

Radio Top

UZH: Log-in-Daten zum Kauf angeboten

Alle Studierende und Mitarbeitende der Universität Zürich (UZH) sind letzten Donnerstagabend über einen laufenden Hackerangriff informiert...

06.02.2023

IT-Markt

Update: Hacker verscherbeln Zugangsdaten zu UZH-Servern für 10 US-Dollar

Cyberkriminelle versuchen aktuell, die Universität Zürich anzugreifen. Diese fordert ihre Mitarbeitenden und Studierenden auf,...

06.02.2023

Hackerangriff: Kein Anschluss unter dieser Uni

30.11.2

Solche

Die Universität Duisburg-Essen ist derzeit nach einem Hacker-Angriff nicht erreichbar.

AZ

Cyberkriminalität: Vice Society stellt Daten der Universität Duisburg-Essen (UDE) ins Dark Web, HAW Hamburg erpresst

Cybererpresser der Ransomware Vice Society hacken zahlreiche Hochschulen und Universitäten, um Lösegeld zu erpressen.

Spiege

17.01.2023

Hacker greifen Unis an: Alle Hochschulen in NRW Ziel von Cyber-Kriminellen

In den letzten fünf Jahren griffen Hacker vermehrt Universitäten an. Die rüsten nun auf – doch eine Hochschulart ist besonders in Gefahr.

MDR

Vermehrt Hackerangriffe auf Hochschulen und Universitäten

Der mutmaßliche Cyberangriff auf die TU Bergakademie Freiberg hat erneut einen Fokus auf die IT-Sicherheit deutscher Hochschulen gelenkt.

RP Online

Uni Duisburg-Essen: Systeme offline - erneut Hacker-Angriff

Im November legte ein Cyber-Angriff die gesamte digitale Infrastruktur der Universität Duisburg-Essen lahm. Die Hochschule baute die Systeme...

14.12.2022

Spiegel

Universität Duisburg-Essen: Daten nach Hackerangriff im Darknet aufgetaucht

Nachdem Hacker zunächst die Systeme der Universität Duisburg-Essen lahmgelegt hatten, erhöhen sie nun den Druck und stellen erbeutete Daten...

17.01.2023

«Defence in Depth» (~2005) – stark reaktiv → Grundschutz

«Generierung verschiedener Sichten»

- **Netzwerk - Zonierung / Architektur**
- IDS / IPS **Entdeckung von «bösartigen» Aktivitäten im Netzwerk / Host's (Host IDS bspw. Alien Vault ~2012)**
- Monitoring (Operative auf Basis Service / Rudimentär auf spezifische Sec. Event's)
- **Security Policies (Baseline resp. Baselinekatalog…..)**
- **Incident Response (Task Force / IT- Notfallmanagement)**
- **Operational Log's**
- **Malwareschutz auf Endpoints**
- **MFA (RSA Token etc.)**
- **Rudimentäre Überwachung AD (PAM / Failed Login etc.)**
- **FIM (File Integrity Monitoring) / CIS (Center for Internet Security) Hardening (OS)**
- **PCI / ISO 27001 /FINMA Rundschreiben /SOX usw.**
- Verschiedene Sichten auf unterschiedliche Systeme auf unterschiedlichen «Monitoren»
- «Beinahe» manuelle Korrelation

Abriss SIEM Entwicklung (2005-2012) eher reaktiv

– **Log Management** entspricht dem Begriff **SIM** (Security Information Management) und steht für die zentrale Sammlung, Übertragung, Speicherung, Analyse und Weiterleitung von Log-Daten aus Netzwerk-Komponenten, Betriebssystemen und Applikationen.

– **SEM** (Security Event Management) übernimmt die Korrelation von Logs anhand definierter Richtlinien, gleicht sie automatisiert mit Standards wie ITIL, COBIT, SOX oder ISO ab und verfügt über Echtzeit-Alarmfunktionen. SEM deckt sich teilweise mit **IDS/IPS** (Intrusion Detection und Intrusion Prevention System).

Ab 2010 – mehr pro Aktiv

– **SIEM** (Security Information and Event Management) vereint die Funktionen von SIM und SEM als Management-Lösung. Es basiert auf unternehmensspezifischen Anforderungen - also auf klaren und umfassenden Definitionen, welche Ereignisse sicherheitsrelevant sind und wie und mit welcher Priorität darauf zu reagieren ist.

→ Korrelation, «Eine Monitoring Übersicht für alles»

SIEM – Security Incident & Event Management (2012)

SIEM Definition

Security Incident and Event Management (SIEM) ist der Prozess der Identifizierung, Überwachung (Umsetzung ISMS etc. –Funktion Grundschutz / entdecken von Anomalien etc.), Aufzeichnung und Analyse von Sicherheitsereignissen oder -vorfällen innerhalb einer Echtzeit-IT-Umgebung. Es bietet einen umfassenden und zentralisierten Überblick über das Sicherheitsszenario einer IT-Infrastruktur.

Paradigm Change: Angenommener Einbruch & Proaktiv statt reaktiv

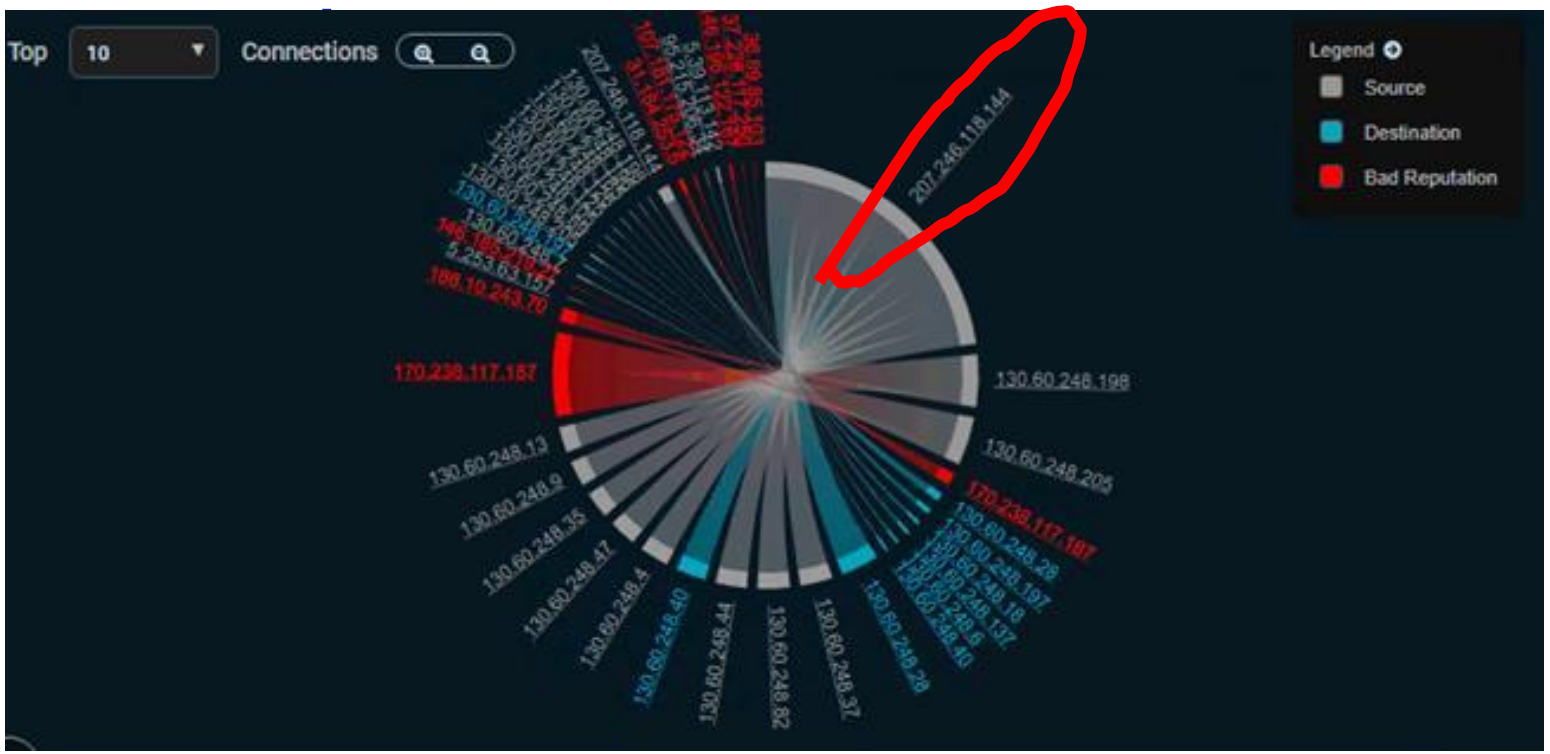
Gegenmaßnahmen, die sich mit der "APT" befassen, müssen unter der **Annahme entwickelt werden**, dass Teile oder alle Sicherheitsmaßnahmen versagen und der **Angreifer die Systeme kompromittiert**. Daher ist es von entscheidender Bedeutung, dass kompromittierte Systeme, sobald sie identifiziert sind, angemessen behandelt werden. Dies ist ein grundlegend anderes Sicherheitskonzept (z. B. ein Basisschutz), bei dem der Schwerpunkt auf **Erkennung und Reaktion statt** nur auf **Prävention** (und nur auf Basisschutz) liegt.*

**Vizualisation*Advanced Persistant Threat*

Process

Additional : «Optimieren der Zufallsentdeckung von Security incident (e.g.«APT»/ Oday etc.)

Erster Einsatz SIEM (oXDR) @ UZH Ransomware Attacke (09.2019) – Threat



- 1 Person / 45 Minuten Ausmass / Massnahmen
- Automatisierung über neu infizierte Clients / Server – Meldung direkt an Admins.
- Schnelle Ländersperrung
- Agent auf Server / Client

SIEM, SOAR, EDR, XDR / oXDR (open Extended Detection and Respons)

- **SIEM (Security Incident und Event Management) → aus SIM & SEM**
  - sammelt Ereignisdaten, erfordert aber manuellen Aufwand(unterschiedliche Tools / Korrelation/ Use Cases)
- **SOAR (Security Orchestration, Automation & Response)**
  - Ansatz zur Verbesserung resp. Beschleunigung (Automation / Effizienz) eines SIEM
  - reduziert manuelle Eingriffe
- **EDR (Endpoint Detection & Response)**
  - EDR, oder Endpoint Detection and Response, sammelt und analysiert auf der Ebene der Endgeräte Anomalien, welche eine Bedrohung darstellen
- **(o)XDR (open Extended Detection & Response)**
  - XDR integriert Untersuchungstools, Verhaltensanalysen und automatisierten Gegenmassnahmen in einer Plattform – Weiterentwicklung von EDR (User Behaviour)

SIEM's – Funktionen (Auswahl Kopie von verschiedenen «Tool's»), Entwicklung ~2023

SIEM:

- EDR (Endpoint Detection & Response)
- XDR / oXDR Open Extended Detection and Response
- **Threat Hunting**
- **Threat Intelligence** Platform (TIP)
- Network Detection & Response (NDR)
- IDS & Malware Analysis
- Security Orchestration and Automated Response (SOAR)

- Syslog
- Server Agent
- User behavior
- API's wie bspw. FW zur direkten Sperrung von IP Adressen (Ingress / Egress) → ~IPS
- Einbindung von Resultaten wie Schwachstellenscanner zur verbesserung der Korrelation
- Playbooks (inkl. Threat Hunting Playbooks)
- KI
- Open API zur Anbindung weiterer Quellen zur schnellen Korrelation von Informationen
- ……..

Wie unterscheidet sich XDR von SIEM?

- XDR ist der Versuch (von Security-Anbietern), die Erkennung von Bedrohungen und die Reaktionszeiten zu verbessern. Die Kategorie wurde 2018 entwickelt und hat 2020 an Bedeutung gewonnen.

  →*Es ist eine starke Verbesserung, bleibt immer noch eine Optimierung der Zufallsentdeckung*

- Verwendungszweck ist aber immer noch der gleiche…..Security Monitoring & Response
- Das Ziel von XDR ist es, alle Sicherheitsdaten und -warnungen zu korrelierten **(API's)** und eine zentralisierte Erkennungs- und Reaktionsfunktion für Vorfälle mit umfassender Überwachung der gesamten Angriffsfläche (Cyberkill Chain) bereitzustellen.
- Daher ist es wichtig, eine XDR-Plattform zu finden, die sich in bestehende Sicherheitskontrollen integrieren lässt oder eine offene Architektur aufweist um diese Integration zu bewerkstelligen.
- Anyway: Es braucht Werkzeuge für die Protokollverwaltung und -aufbewahrung sowie die automatische Erkennung von Security Event's und Reaktion auf Bedrohungen.

  →Die gewählten Lösungen müssen **integriert**, konfiguriert und **feinabgestimmt** werden, um Sicherheitsvorfälle effektiv und effizient zu erkennen und darauf zu reagieren.

Universität Zürich[UZH]

Zentrale Informatik

Wege zu einem Security Monitoring & Response (SIEM / XDR / Org. etc.)

Entdecken - aktiv

entdecken

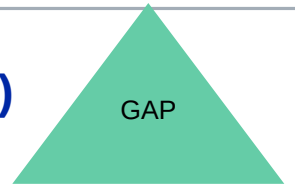
- auf die Spur kommen
- auffinden
- aufspüren
- aufstöbern
- ausfindig machen
- ermitteln
- finden
- erkennen
- feststellen
- …..

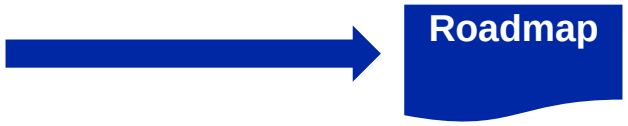
Analyst (SOC - Team) & Werkzeug

Schutzmassnahmen mit Standards (Cyber Security Framework, 2014)

Identifizieren	Schützen	Entdecken und Reagieren	Wiederherstellen
Identifizieren und schaffen relevanter Grundlagen • Inventar (Asset Management) • Risiko Management • Governance	**Grundschutz** • Schutzmechanismen für kritische Infrastrukturdienste • Angriffe verhindern oder zumindest die Auswirkungen reduzieren • Zugriffskontrolle • Patch-Management • Technische Schutzmechanismen wie Virenschutz oder Firewalls • Awareness und Training • Prozesse und Prozeduren für die Systemwartung	**Entdecken** • Die Fähigkeit wichtige, sicherheitsrelevante Ereignisse und Anomalien zeitnah entdecken zu können **und Reagieren** • Bei einem Ereignis das Risiko einzuschätzen, entsprechend zu handeln und/oder zu eskalieren	**Betriebliche Kontinuität** • Pläne und Verfahren zur raschen Wiederherstellung von betroffenen Services • Business Continuity & Recovery Planning • Wiederherstellungsverfahren • Kommunikation

Scope SIEM (Integration SIEM /XDR)





28500 Studenten
~9700 Mitarbeiter

Cyber Security Riskassessment

Identification

- "IT – Risk View"
  - IT – Risk / Threat
  - Identification of "UZH - Crown Jewels"

Risk= Asset *Threat * Vulnerability

Cybersecurity Readiness @ UZH

APT

Respond

Detect

- "Attack View"
  - Incident Respond Capabilities
  - Detection Capabilities / SIEM
  - Account Monitoring and Control
  - Malware Defenses / APT Malware Strategy
  - …

Schwerpunkt

CIS Critical Controls

SIEM Perspektive: Mengengerüst (Anzahl / Grösse in GB etc.

Grundschutz

Protect

Recover

- "IT – Grundschutz View"
  - Policies / Directives
  - Anti-Malwarekonzept
  - Datensicherheitskonzept
  - Management Tools (bspw.Vulnerabililty Management (CERT)
  - Softwareentwicklungslebenszyklus
  - Inventory of Authorized and Unauthorized Devices
  - Secure Configurations for HW/SW
  - BCM
  - …..

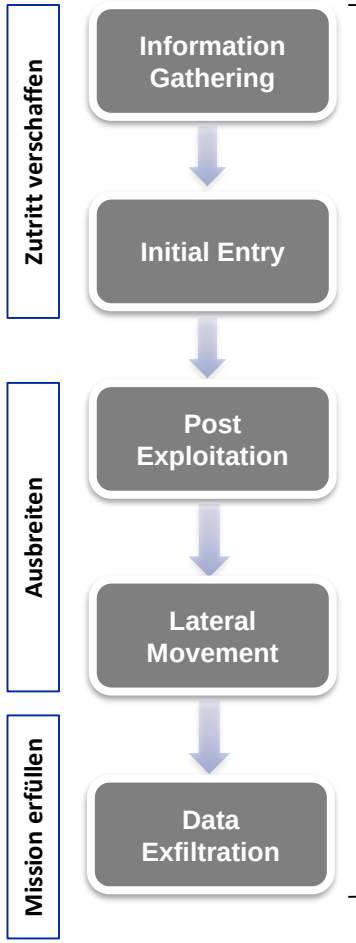
ISO 27001

NIST

…..

CIS – Controls (Bsp. Cyberattacke «APT») (Advanced Persistent Threat = gezielte, länger andauernde, unentdeckte Angriffe)

Cyber Attack Chain



«SIEM»

SANS Critical Control Catalog for Cyber Security Defense (CIS) / NIST

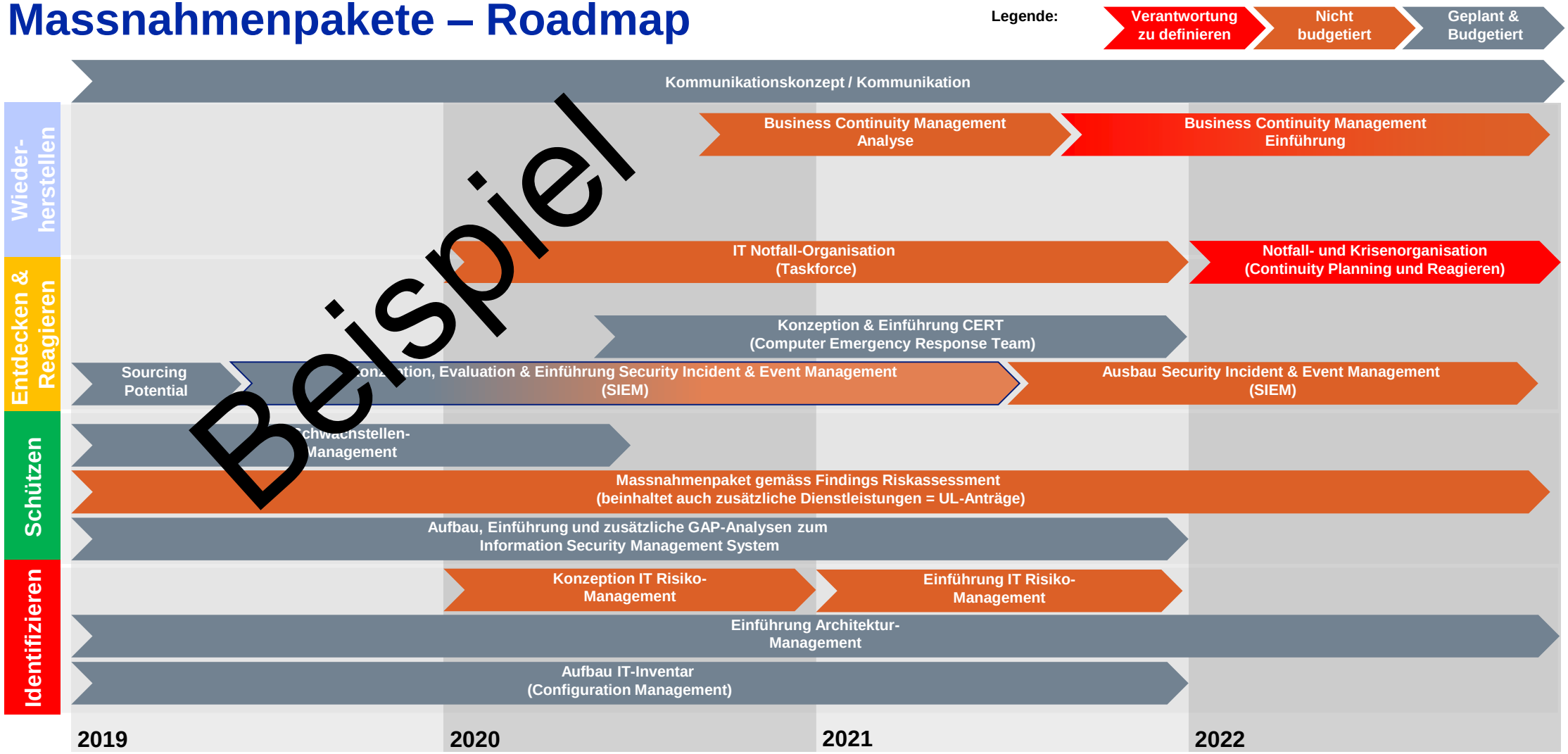
1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for HW/SW
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management (incl. Forensic)
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

Prioritization of the main SANS Controls to strengthen Cyber Security Defense @ UZH

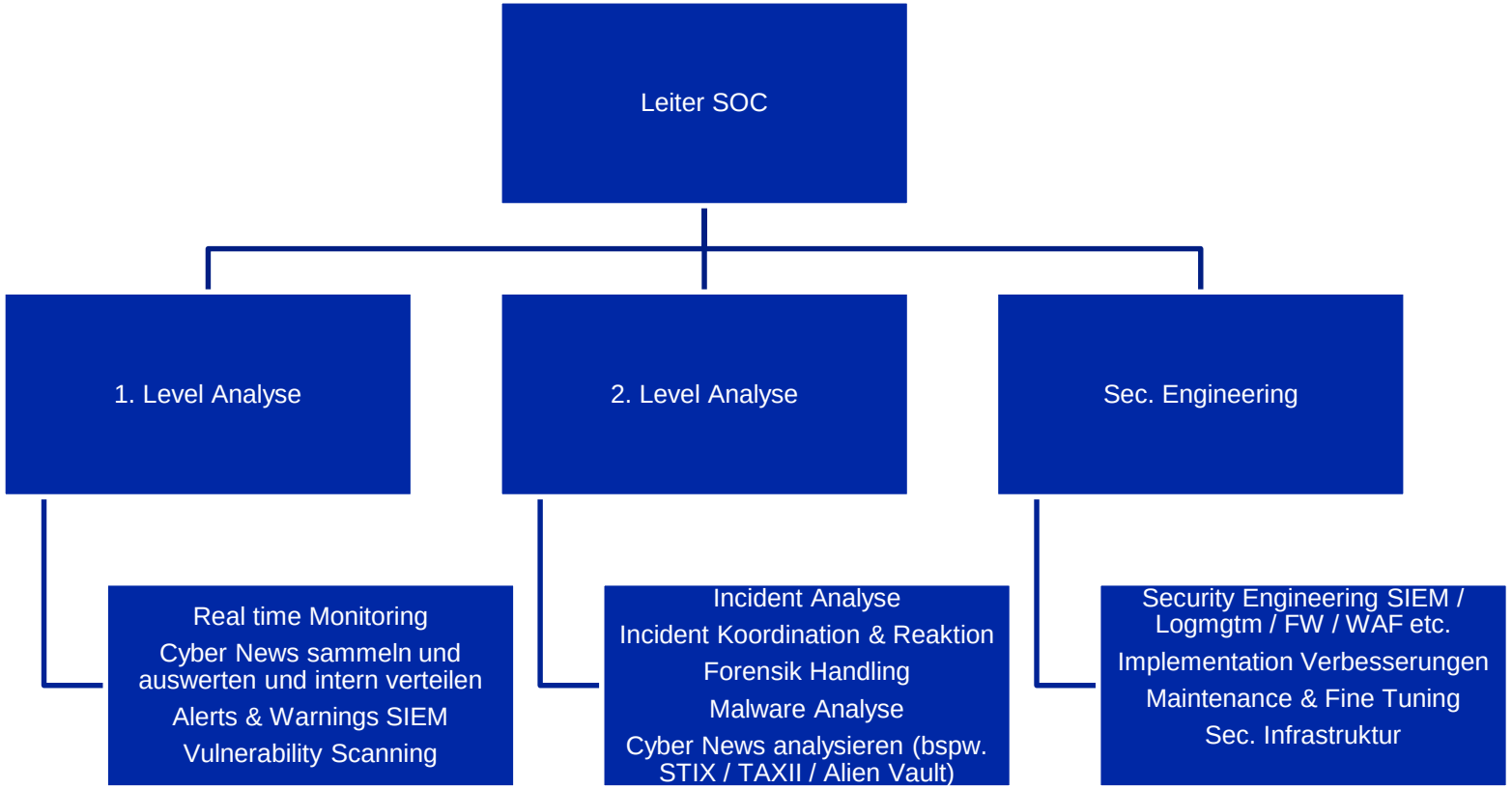
Prio.	Control
1	14: Maintenance, Monitoring, and Analysis of Audit Logs — Schützen — Entdecken und Reagieren
2	18: Incident Response and Management (incl. Forensic) — Entdecken und Reagieren
3	5: Malware Defenses
4	2: Inventory of Authorized and Unauthorized Software — Schützen
5	16: Account Monitoring and Control — Entdecken und Reagieren
6	12: Controlled Use of Administrative Privileges — Schützen
7	17: Data Protection — Schützen

Massnahmenpakete – Roadmap

Abgeleitet aus Assessment (siehe Folie 18)

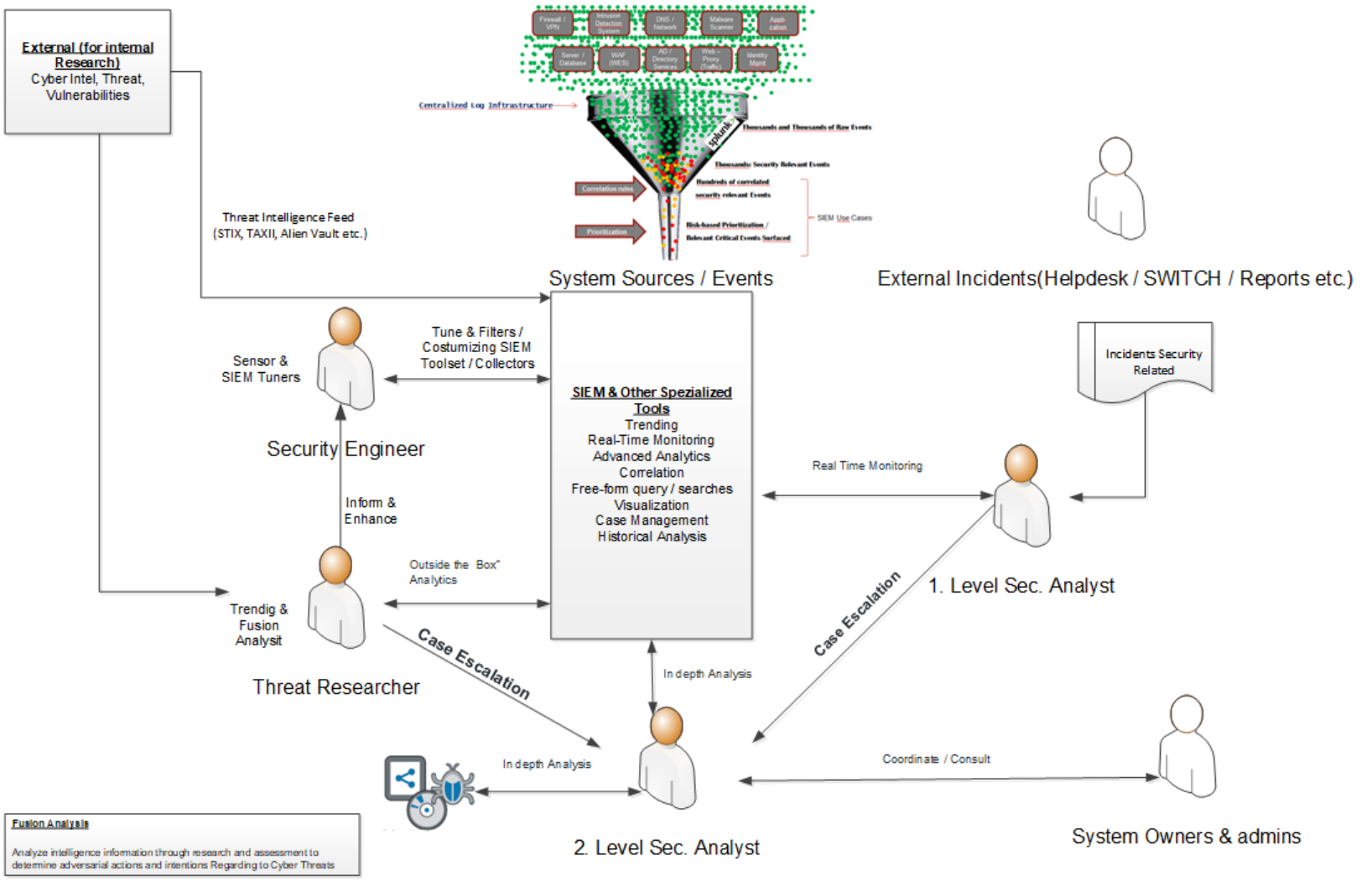


Soc Org. kleines SOC

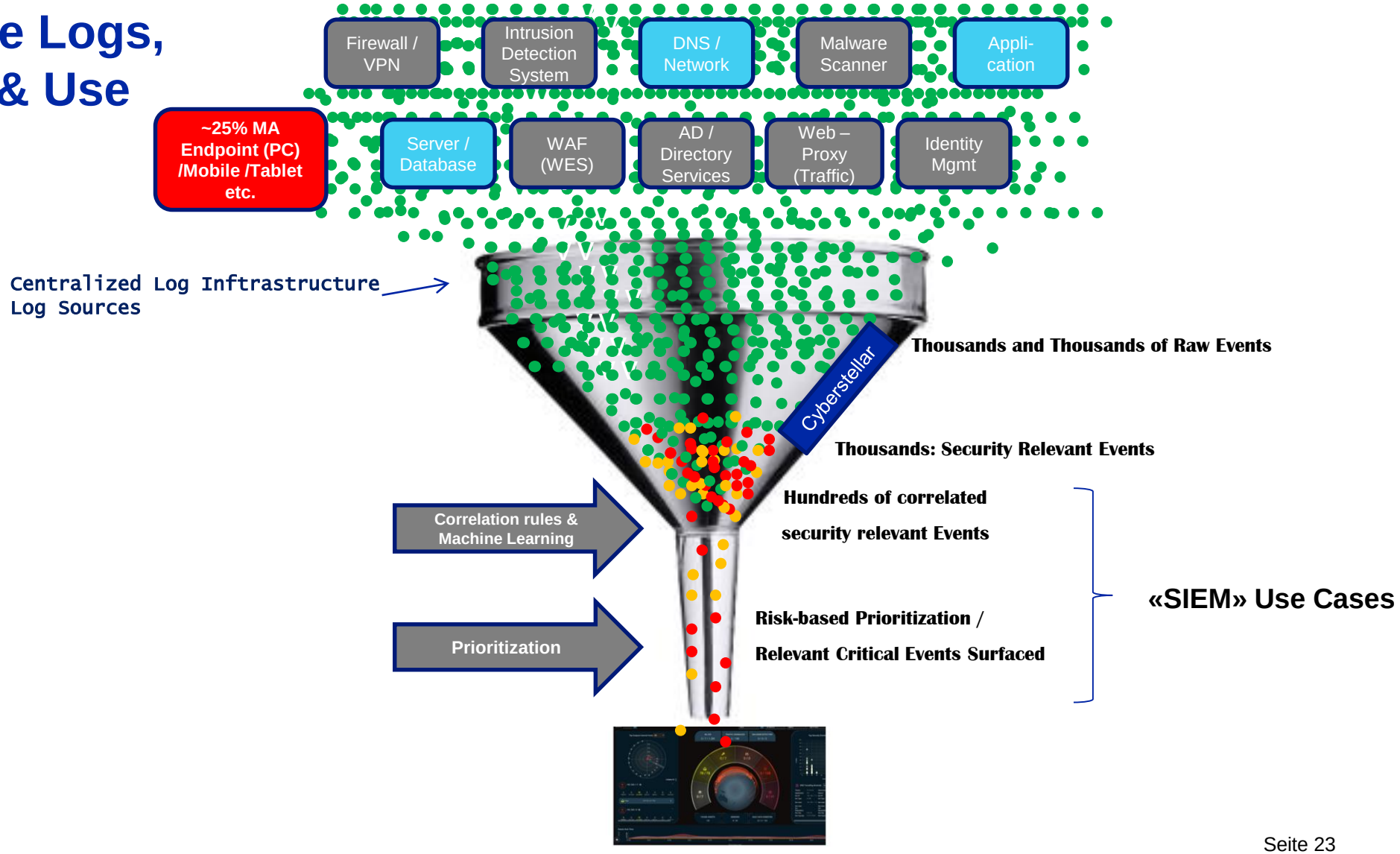


One Note / Mitre

SIEM – Rollen


External (for internal Research)
Cyber Intel, Threat, Vulnerabilities
Threat Intelligence Feed (STIX, TAXII, Alien Vault etc.)
Centralized Log Infrastructure
Thousands and Thousands of Raw Events
Thousands Security Relevant Events
Hundreds of correlated security relevant Events
Risk-based Prioritization / Relevant Critical Events Surfaced
SIEM Use Cases
System Sources / Events
External Incidents(Helpdesk / SWITCH / Reports etc.)
Sensor & SIEM Tuners
Tune & Filters / Costumizing SIEM Toolset / Collectors
SIEM & Other Spezialized Tools
Trending
Real-Time Monitoring
Advanced Analytics
Correlation
Free-form query / searches
Visualization
Case Management
Historical Analysis
Incidents Security Related
Security Engineer
Inform & Enhance
Real Time Monitoring
Outside the Box" Analytics
Trendig & Fusion Analysit
Threat Researcher
Case Escalation
1. Level Sec. Analyst
In depth Analysis
Case Escalation
In depth Analysis
Coordinate / Consult
2. Level Sec. Analyst
System Owners & admins
Fusion Analysis
Analyze intelligence information through research and assessment to determine adversarial actions and intentions Regarding to Cyber Threats

Security relevante Logs, Realtime Events & Use Cases (Mitre ORG)



IT – Security Monitoring Infrastructure

SWITCH → INTERNET

O365

150 Institute mit eigener IT

Institution X

Institution N..

Institution Y

Institution Z

Zone X

Zone Y

Zone Z

Zone …

Network of the University of Zurich

Core Datacenter Traffic

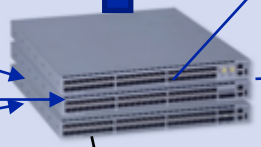
Copy of all Core Datacenter Interzone Networktraffic

Kerninfrastruktur

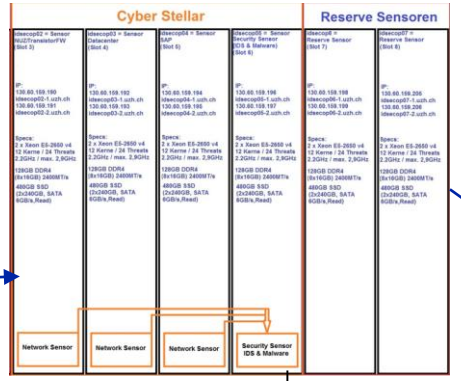
Aggregation – Filtering (Protocol / Port / IP / Pakettype etc.)

~~Netflow Data~~

Copy of all Network Traffic



Aggregation (Switch) Infrastructure

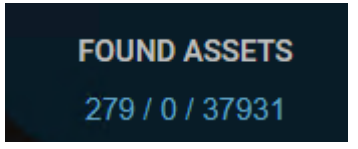


Syslog FW - Filtered

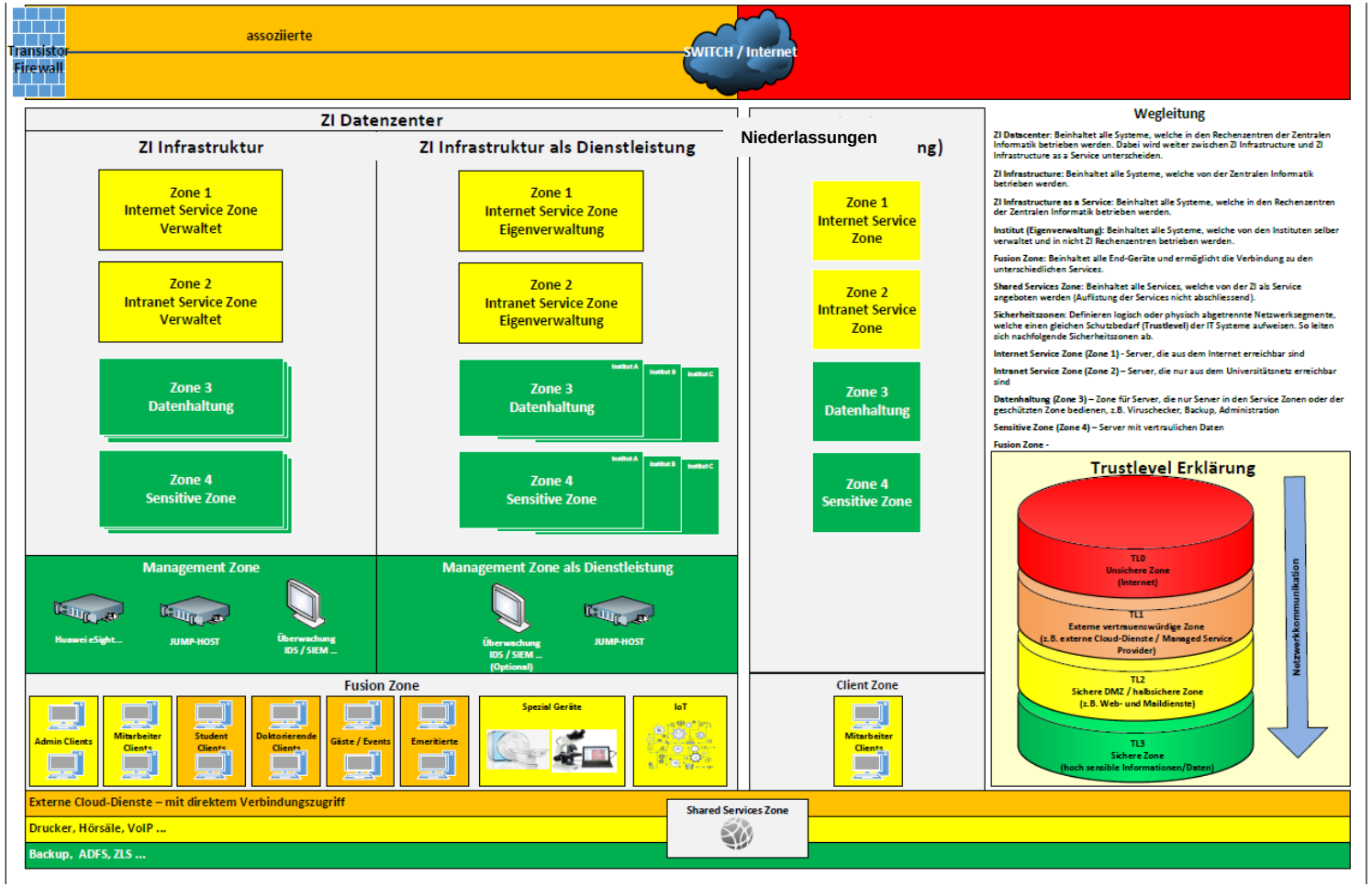
Syslog - Server

Server - Syslog – Core Datacenterzone

kibana



Defence in Depth



Cyberattacke erkennen und reagieren (UZH) – Kein reiner Tool Ansatz –

Trotzdem starten die meisten mit dem Tool (SIEM ist aber als Framework zu verstehen)

- **Assessment** – Übersicht schaffen was ist wichtig! (Monitoring Priorität)
- **Task Force** & internes CSIRT(mit Spezialisten)/ Notfallstab / Krisenstab inkl. Übungen / Technische Test's (Pentest / Cymulate etc.)
- **Play Book** (Cyberattacke / Ransomware / Malware etc.)
- ***Compliance*** (Büpf / ab September '23 Bundesrat überweist Botschaft zur Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen – UZH resp. Hochschulen gelten als kritische Infrastrukturen)
- **Kommunikationskonzept Cyberattacke / Einbindung externer Spezialisten (Polizei / Spezialisten welche mit Verbrecher verhandeln können etc.)**
- **Externe Sichten auf die eigene Organisation** (Balanced Score Card / Black Kite / Have been pwnd etc.)
- **EDR** (Endpoint Detection & Response / Agent auf Endpoint).
- **Threat Hunting / Intelligence (Generierung von IOC aus bekannten Cyberattacken, stix / taxi)**
- **Werkzeuge** (SIEM resp. oXDR (Use Cases / SIEM Infrastruktur / Quellen & Eigententwicklungen / Automation → Effizienz)

→SIEM Use Cases (2023……sollten schon die meisten in einem SIEM hinterlegt sein ☺ → MITRE)

Fragen?

Fragen !