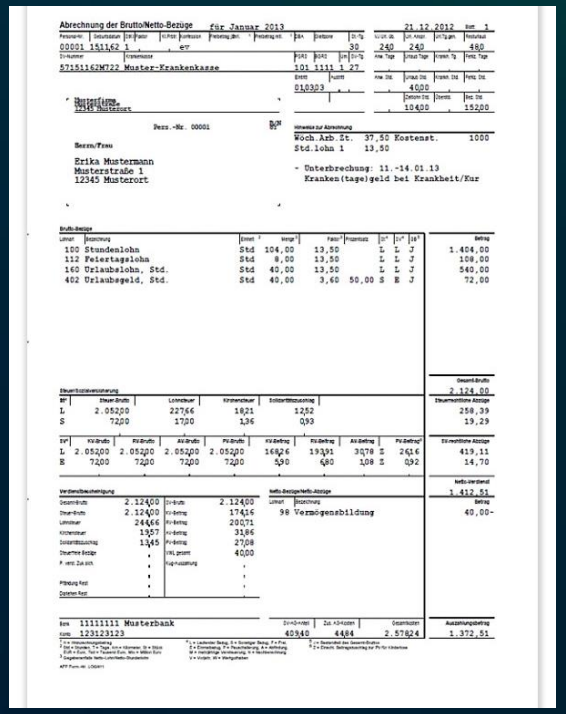
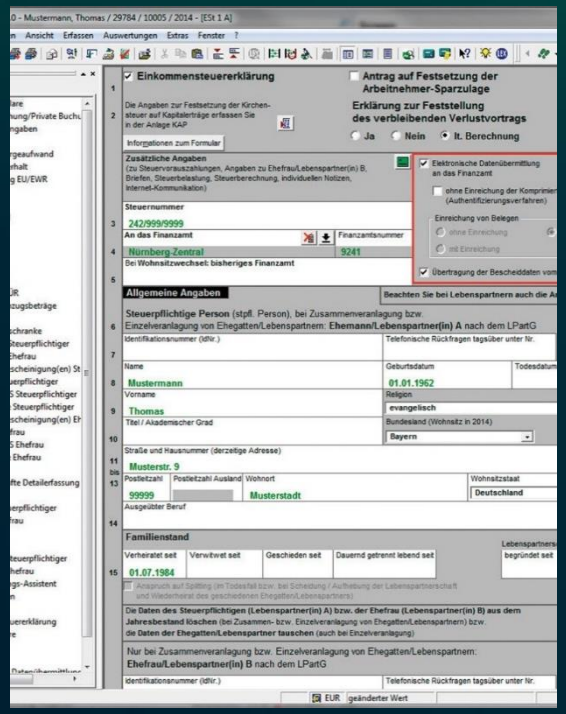
Security Operation Center

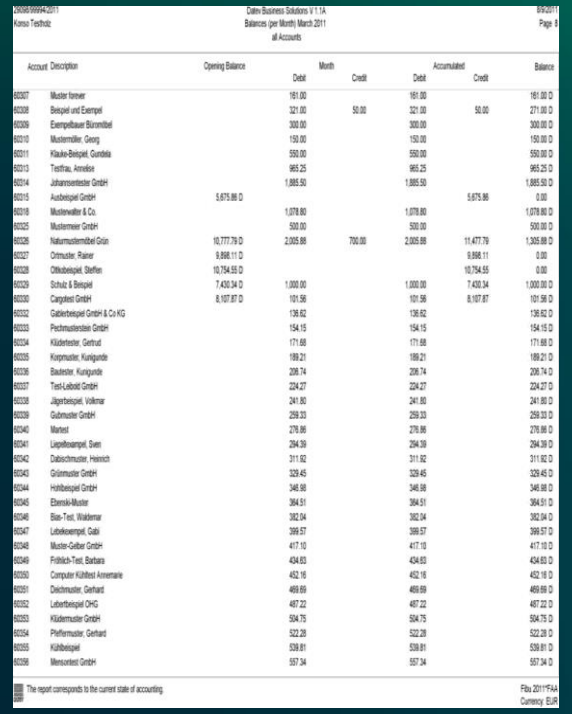
Wie wird DATEV wahrgenommen … ?



Gehaltsabrechnung



Steuererklärung



Business Reports

Presse

Gefahrenlage

Infizierte - E-Mails - pro Tag (blocked)

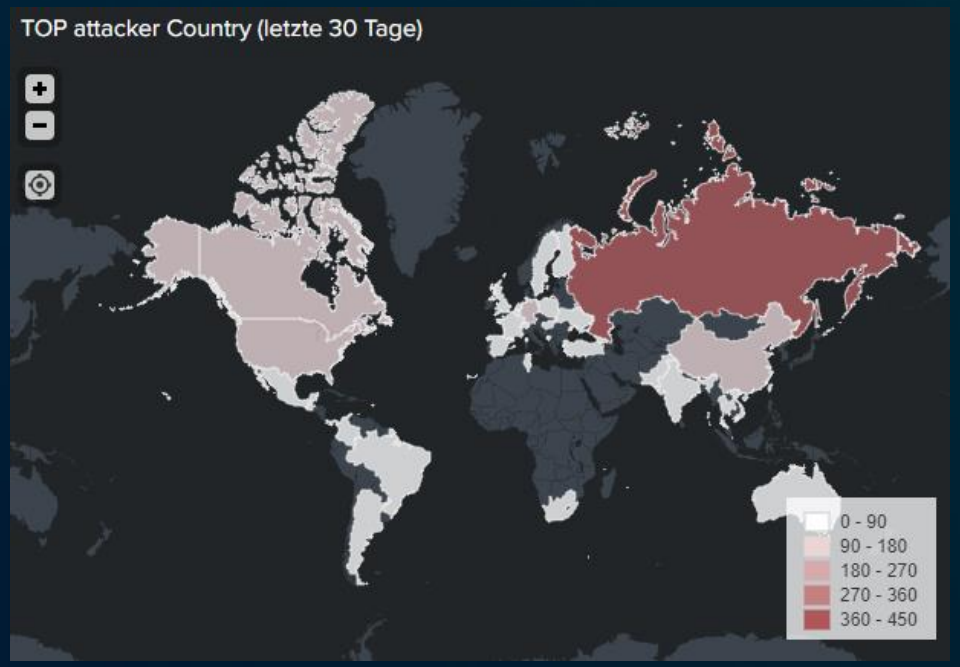
420 ↘ -143

SPAM- E-Mails - pro Tag (blocked)

126 459 ↗ 9 688

Netzwerkangriffe pro Tag

818 624



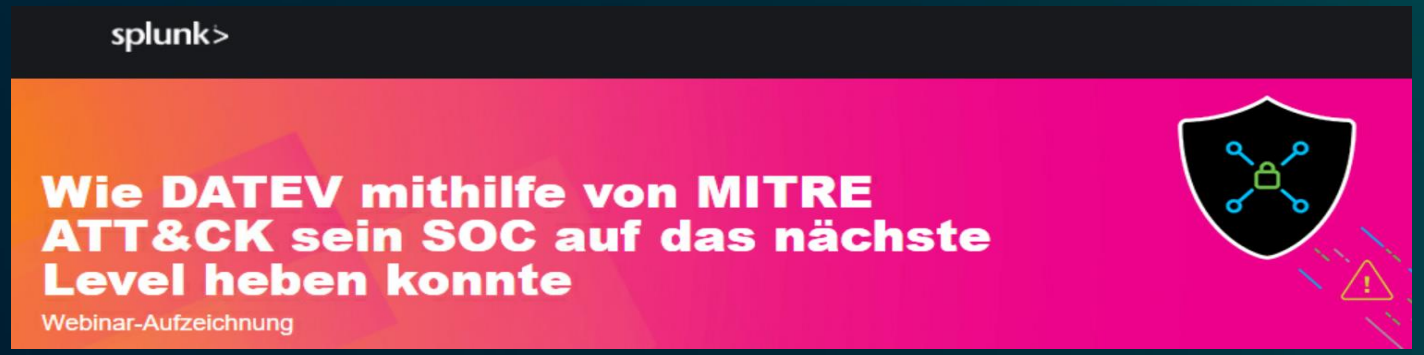
13

schwerwiegende Vorfälle im Jahr 2021

‚die eine intensive Analyse
des SOC Teams forderten,

wurden erfolgreich abgewehrt!

Detaillierte Informationen



https://conf.splunk.com/files/2019/slides/SEC1411.pdf

SOC Services

Vorfall / Major - Combat Mode

SIEM
Detection, Analyse, Incident Response

Ohne SOC SIEM Service
Fachabteilung alleine verantwortlich für die Anomalie Erkennung und Meldung an das SOC !!!

SOC Services (Überblick)

Organisatorische Anweisung durch SPF

SIEM

01

Vorfall / Major

Außergewöhnliche Sec Vorfälle / Major, IT-Notfall, Krise

02

Detection

Anomalien erkennen, anhand Angriffsmuster in Splunk Logs

03

Analyse

Analyse der Auffälligkeiten. War der Angriff erfolgreich?

04

Response

Gefahreneindämmung und Maßnahmen einleiten, um auf Vorfälle zu reagieren

Voraussetzungen Einweisung im Umfeld + AP
Empfehlung Logs in Splunk und lesender Zugriff auf Security Tools & Werkzeuge

Voraussetzungen Logs in Splunk + Ablauf der 3 Phasen und damit die Umsetzung der nötigen Maßnahmen in den Prozessen und Werkzeugen

SOC Services (Detail)

SIEM

01

Vorfall / Major

Logs im Splunk **empfohlen**

Security Vorfälle fachliche Steuerung / Consulting durch den Major + **Analyse / Forensik** falls möglich + Koordination mit externen Partner und Unterstützung der FA

Verantwortung und Entscheidungen liegen im **Management** (Major)

02

Detection

Voraussetzung
Normalisierte Logs im Splunk

- Alarmierung auf Grundlage der Splunk Logs wird aufgebaut
- Anomalie-Erkennung
- **UseCase Playbooks** werden erstellt

03

Analyse

Voraussetzung
Zusammenarbeit, Technischer Zugriff + Prozess

- Daten von Systemen werden live oder offline im SOC Umfeld / Labor analysiert
- Beispiele: ISO, RAM Snapshots, Scripte, malware file Analyse...
- **Analyse Playbooks**

04

Response

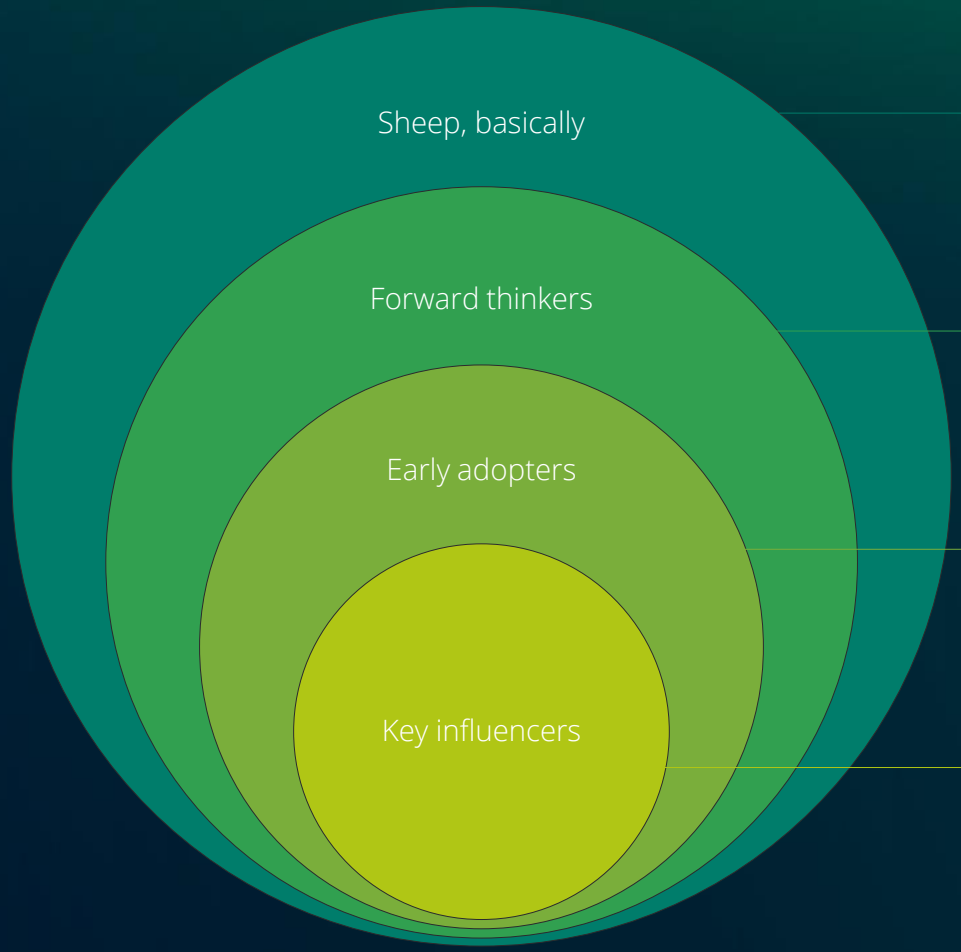
Voraussetzung
Abstimmung Prozess

- Auf Alarme reagieren
- Dokumentation und Abstimmung mit Fachabteilungen
- Beispiele: Prozess Kill, Isolierung, FW blocking, Port down...
- **IR Maßnahmen**

Beispiele

Angriff	02 Detection Playbooks	03 Analyse Analyseplaybooks	04 Response IR-Playbooks
Intern -> Intern	Pass the Hash User Credentials erbeutet	• AD Analyse • AP kontaktieren • Server Analyse • Netzwerk Analyse DNS,FW,Proxy…	➢ User sperren ➢ VPN terminieren ➢ Prozess terminieren
Extern -> Intern	Webangriff	• Angriff verstehen • Vulnerability überprüfen • System Analyse intern • AP kontaktieren • Extern Quelle analysieren	➢ Blocking FW ➢ DDoS mitigation ➢ Rule WAF / IDPS ➢ Backup / Restore

SIEM Logquellen Prio



Anwendungslogs
Webserver-Logs, Datenbanken, Programme,...

Vulnerability / Hilfsmittel
Vuln-Scanner, Asset-, Patch-Datenbanken,...

Client / Server
Security-, System-Logs, AD-Logs

Netzwerk / Security Tools
Routing, DNS, FW, IDPS, WAF, ...

SIEM Logquellen

Server
-Win Security event logs
-Linux Logs auth
-AD/DC
- IDP (IdentityLogs)
...

Clients
-Cloud Defender
-Cloud Identität user
...

Security Tools
- ATA
- FW
- EDR
- IDS
- Proxy
- AV
- WAF
...

Netzwerk
- dns
- routing
- dhcp
- Vpn
- Loadbalancing
...

Hilfsmittel in Splunk
- Ucmdb
- QIP
- wsus (patches)
- Changes
....

Service/Anwendungslogs
- Webserverlogs (Apache)
- Mail
- Esx
...

Vulnerability
- Tenable
- Qualys
...

Für das SOC nötige unterstützende Prozesse/Services

-Assetverwaltung / Geräteinventar

-Patchmanagement / Softwareinventar

-Vulnerabilitymanagment

-Change/Incidentmanagement

-Penetrations Prozess

-Infrastrukturdokumentation (Netzpläne...)

-Riskmanagement (Risk2Val)

-Artefakt Handling & Transport

Zusätzliche externe Prozesse/Informationen für das SOC-Team, die sich als sinnvoll erwiesen haben

- Enge Zusammenarbeit mit SOCs (Diehl, Mediamarkt, etc.)
- Lagebildbewertungen durch BSI, aber auch Zukauf aus kommerziellen Quellen (z.B. dcso.de)
- Zukauf von externer Beratungsleistung
- Virtuelle Trainings der Security-Analysten (z.B. rangeforce.com)
- Schulungen bei Trainingsanbietern wie ISH (Information Security Hub, ish-muc.com)

UseCase: von der Idee zur Fertigstellung

Idee an das SOC

Klärung:
- Ziel des UseCases
- Verantwortlichkeiten bei Alarm
- Reaktion bei Alarm

Daten in SPLUNK verfügbar

- QS
- Aktivierung der Ticketerstellung
- Automatisiertes Reporting Betriebsrat

Implementierung im DATEV-SIEM-Framework

- Permanentes False-Postive-Tuning
- Automatisiertes Reporting der Tickets

UseCase Produktiv SOC-ServiceDesk 7/24 erreichbar

Allgemeine zeitliche Einschätzung

Alle Angaben sind ein Durchschnitt aktueller Erfahrungen und können je Logquelle oder UseCase stark variieren

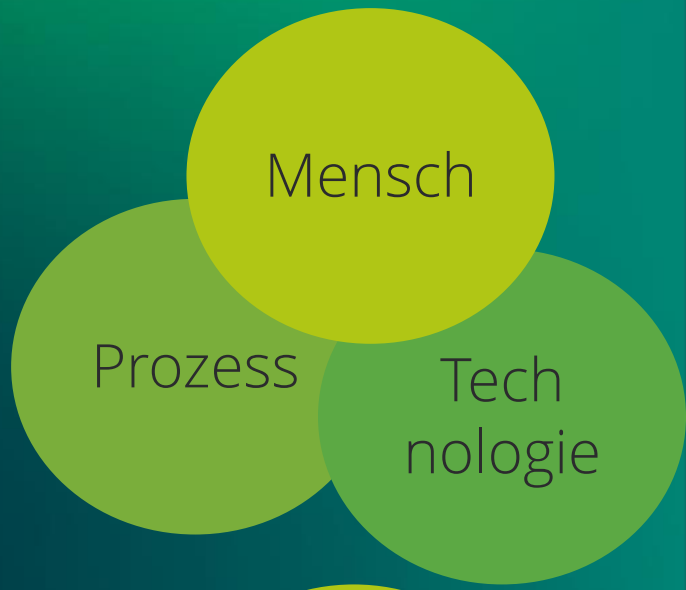
- Eine neue Logquelle
  - Pro Logquelle min. 1Woche
  - Normalisierung der Logs ca. 4 Wochen
- Ein neuer UseCase
  - **UseCase** in Splunk entwickeln : 2-4 Wochen Warum? Normalisierung whitlisting, tuning
  - **Analyse**: Pro UseCase mehrere Meetings und Abstimmungsrunden
  - **Incident Response**: Pro Usecase mehrere Meetings mit Abstimmung
- Scripte/Tools:
  - 2-3 Monate bei neuen Entwicklungen/Umgebungen

Herausforderungen SOC

Mensch: Hohes Maß an Schulungs- und Trainingseinheiten

Prozess: Zusammenarbeit & Beratung mit Fachabteilungen und Koordination - der Beratungsanteil nimmt stetig zu

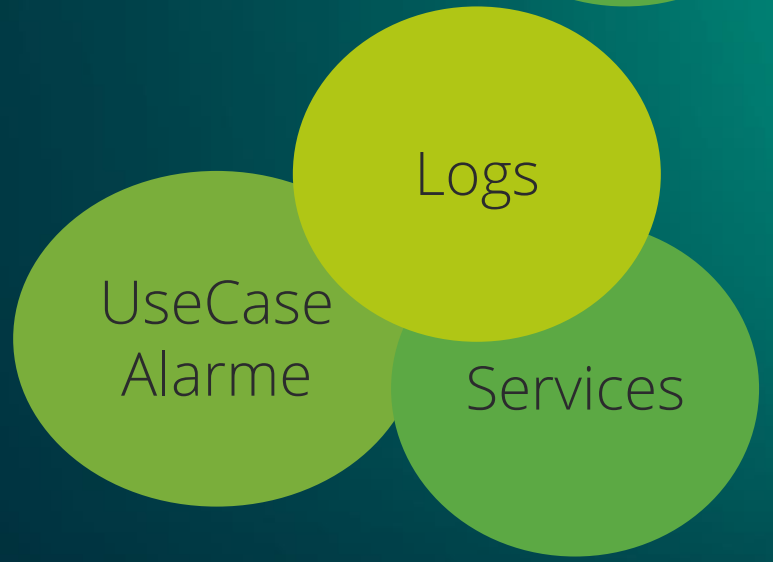
Technologie: Komplexe IT-Strukturen im Unternehmen



Logs: Voraussetzung zur Visibilität von Angriffen

UseCases/Alarme: Vorfallserkennung und Bearbeitung der Fälle

Dienstleistung: Unterstützende Funktionen für Beratung + Verbesserung der Gesamtsicherheit und Resilienz



Ein SOC ist kein Trend,

es ist inzwischen überlebenswichtig,

in der heutigen Zeit und der steigenden Gefahrenlage.

Haben Sie noch Fragen

Gerne auch Feedback

Zukunft gestalten. Gemeinsam.

Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

May 2021 – https://aka.ms/MCRA

Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

Azure Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Azure & 3rd party clouds | Endpoint & Server/VM | Office 365 Email and Apps | Identity Cloud & On-Premises | SaaS Microsoft Cloud App Security | Other Tools, Logs, and Data Sources

Extended Detection and Response (XDR)

Azure Defender — **Microsoft 365 Defender**

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF

Software as a Service (SaaS)

Microsoft Cloud App Security

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Microsoft Endpoint Manager
Unified Endpoint Management (UEM)
Intune | Configuration Manager

Microsoft Defender for Endpoint
Unified Endpoint Security
- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Azure Security Center – Cross-Platform Cloud Security Posture Management (CSPM)

Secure Score | Compliance Dashboard

On Premises Datacenter(s) | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet: NGFW | Edge DLP | IPS/IDS | Azure AD App Proxy *Beyond User VPN*

Intranet: Azure Arc | Azure Stack

Express Route | Private Link

Azure Marketplace

- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- *Security & Other Services*

Information Protection

Classification Labels

- Azure Purview
- Microsoft Information Protection (MIP): Discover, Classify, Protect, Monitor
- File Scanner *(on-premises and cloud)*
- Data Governance
- Advanced eDiscovery

Compliance Manager

Azure Active Directory

Passwordless & MFA
- Hello for Business
- Authenticator App
- FIDO2 Keys

Identity Protection
- Leaked cred protection
- Behavioral Analytics

Azure AD PIM

Identity Governance

Azure AD B2B & B2C

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 Security

Network protection | *App control*
Credential protection | *Exploit protection*
Full Disk Encryption | *Behavior monitoring*
Attack surface reduction | *Next-generation protection*

IoT and Operational Technology (OT)

Azure Sphere

Azure Defender for IoT
- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

Azure Defender – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)