Tech Data
Advanced Solutions

LOGPOINT SIEM & UEBA

IT Sicherheit erhöhen & Compliance schaffen!

*Security Information and Event Management

*User and Entity Behavior Analytics

Wolfgang Rieger

Senior Business Development Manager DACH
Security & Mobility & Analytics & IoT & Services

SIEM & UEBA – lassen Sie sich informieren

was in Ihrem Netzwerk geschieht!

Vertrieb = CRM Kaufleute = ERP

Security = SIEM

TechData Advanced Solutions

Welche Bereiche sind SIEM & UEBA relevant im Unternehmen?

Das Firmengelände	Die Mitarbeiter	Das IT Netzwerk	Die Kontrollinstanz	Die Management-instanz
				
Zugangskontrolle	Sicherheitstraining	NGFW, Proxy, APT-Security, Sandbox, NW-BA	Security Monitoring	Risikoanalyse und Risikomanagement
Produktion (IoT & OT)	IAM & PAM	Client- / Server APT-Security	Security Information and Event Management (SIEM)	Change Management
Videoüberwachung	User Governance	Vulnerability & SW-Patch-Management	Angriffsanalyse, Verteidigung	Prozessautomation
Luftraumüberwachung	UEBA	Mobile Security (MDM, EMM, MTD,MTM)	App Security	Krisenmanagement

TechData Advanced Solutions

Tech Data
Advanced Solutions

Warum ist SIEM & UEBA gerade jetzt so wichtig?

Wer wacht über Home und Mobile Worker

Bereits vor der globalen Krise hatte das Arbeiten von Zuhause Vorteile

86% der Beschäftigten sind der Meinung, dass das Arbeiten von Zuhause den Stress deutlich reduziert.

Firmen, die Ihren Mitarbeitern erlauben von Zuhause aus zu arbeiten, haben bis zu 25% weniger Fluktuation als solche, die das nicht erlauben

Voraussichtlich haben bis 2028 73% aller Abteilungen remote Arbeitsplätze.

Quelle: FlexJobs The State of Telecommuting, 2017; Owl Labs The State of Remote Work, 2018, Upwork Future Workforce Report, 2019

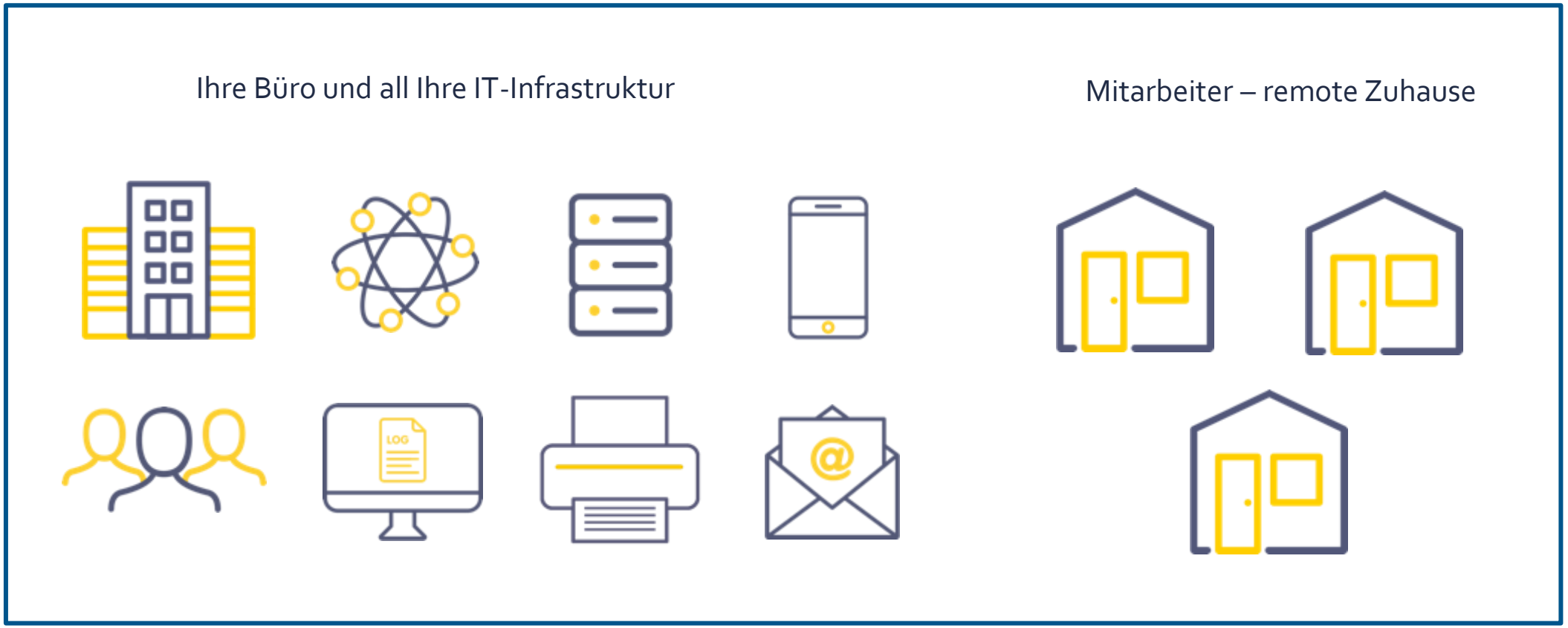
6

Warum gerade jetzt SIEM/UEBA so wichtig sind

Ihre Büro und all Ihre IT-Infrastruktur – Alles befindet sich innerhalb Ihres Netzwerks

Warum gerade jetzt SIEM/UEBA so wichtig sind

Sobald Mitarbeiter remote arbeiten und sich außerhalb des geschützten Netzes befinden, müssten Sie den Perimeter erweitern



Warum gerade jetzt SIEM/UEBA so wichtig sind

Sobald Mitarbeiter remote arbeiten erweitert und erweitert und erweitert sich Ihr Perimeter.

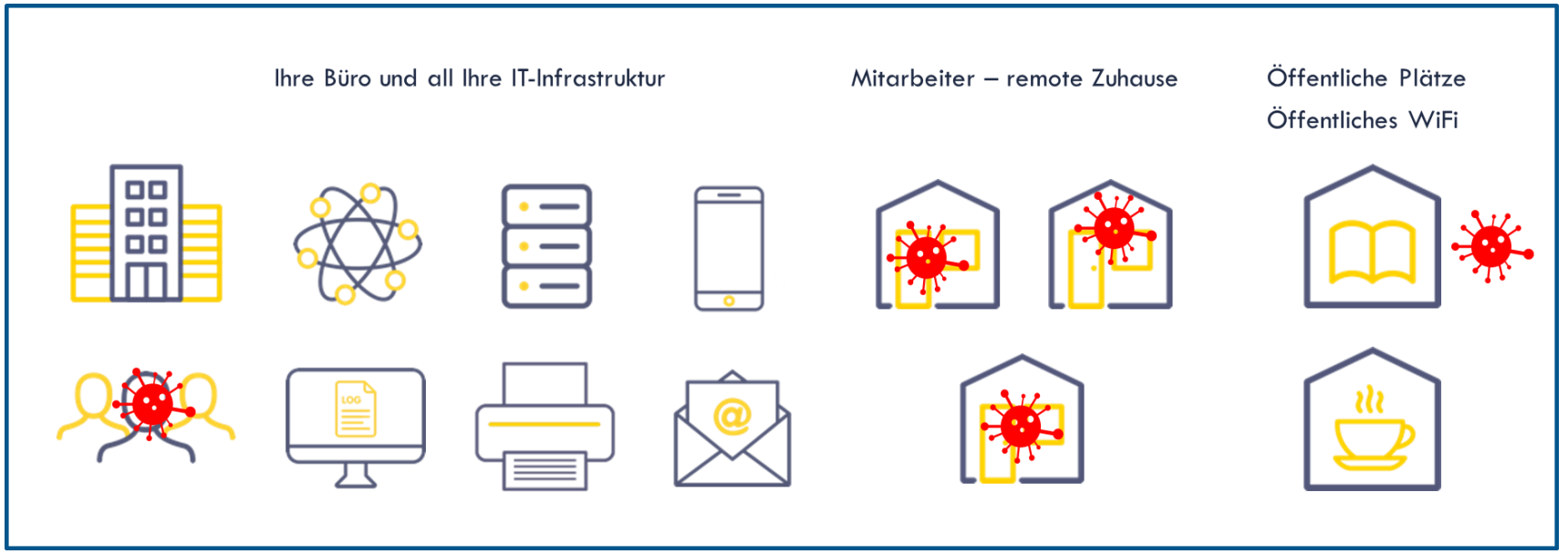
Ihre Büro und all Ihre IT-Infrastruktur

Mitarbeiter – remote Zuhause

Öffentliche Plätze
Öffentliches WiFi

Warum gerade jetzt SIEM/UEBA so wichtig sind

Sobald Mitarbeiter remote arbeiten erweitert und erweitert und erweitert sich Ihr Perimeter.



- ✓ Klassische Perimeter Security ist hilflos
- ✓ Sie benötigt eine Lösung die das Netzwerk monitort und das
- ✓ Verhalten Einzelner und Gruppen auf Anomalien hin untersucht

SIEM & UEBA wachen inner- **UND** außerhalb Ihres Netzwerkes

TechData Advanced Solutions

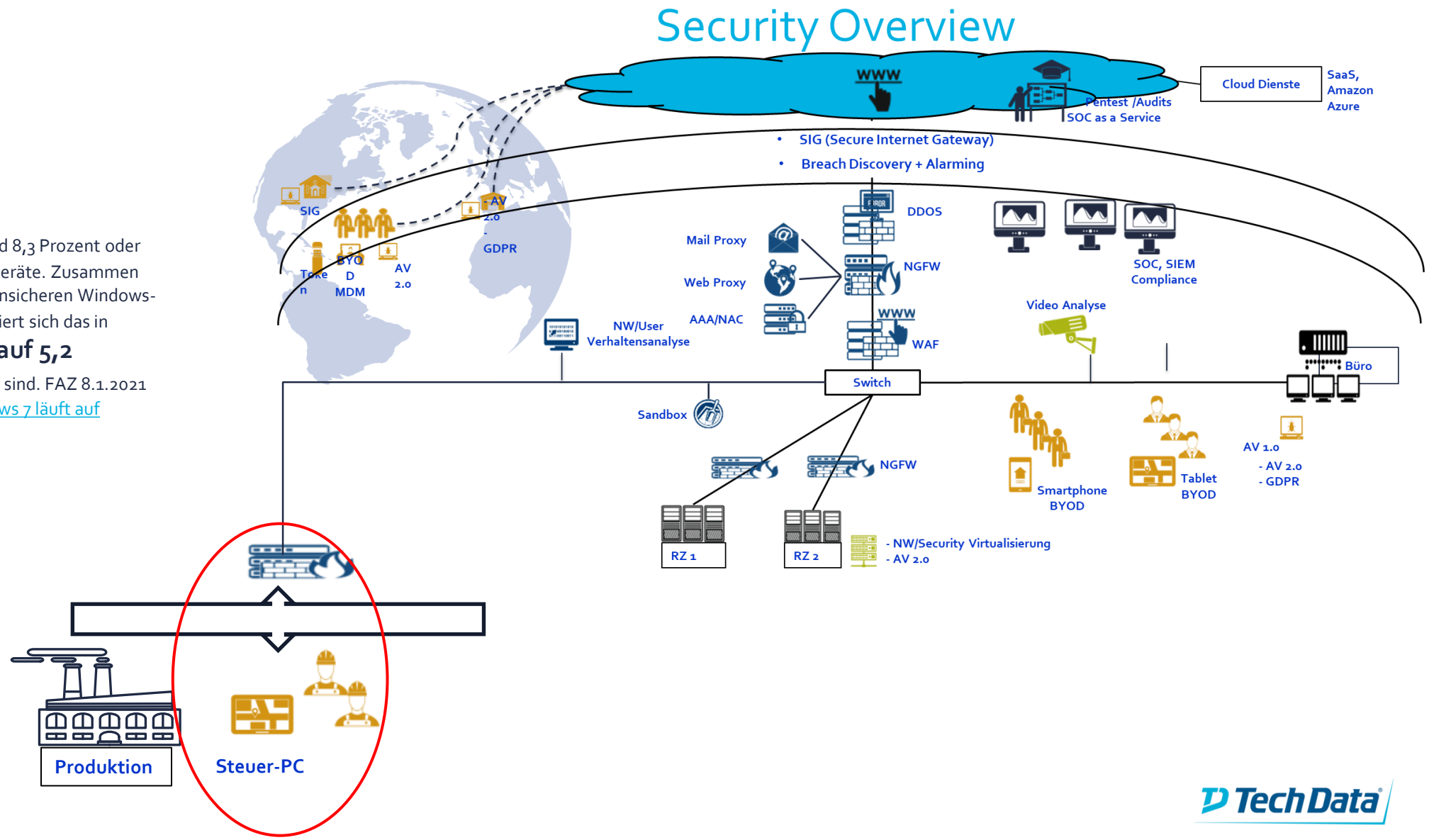
Tech Data
Advanced Solutions

Welche neuen Herausforderung kommen auf Sie zu?

Cyber & I-OT Security – Sicherheitsgesetz 2.0

SIEM/UEBA

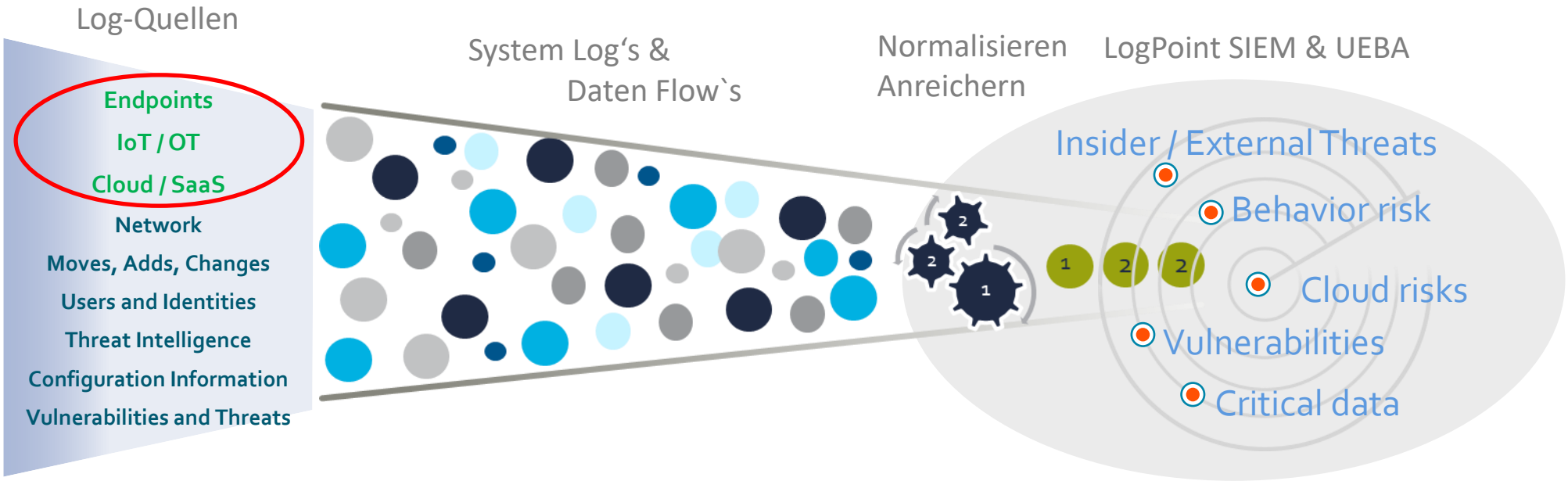
Statcounter verzeichnet dabei rund 8,3 Prozent oder gut vier Millionen **Windows-7**-Geräte. Zusammen mit den ebenfalls veralteten und unsicheren Windows-Versionen **Vista, XP und 8** addiert sich das in Deutschland aber immerhin noch **auf 5,2 Millionen** Geräte, die unsicher sind. FAZ 8.1.2021
[Veraltetes Betriebssystem: Windows 7 läuft auf Millionen Computern (faz.net)]



Wie funktioniert SIEM & UEBA?

Warum werden Endpoints, IoT und OT häufig nicht berücksichtigt?

SIEM wacht inner-/außerhalb der Perimeter-Security

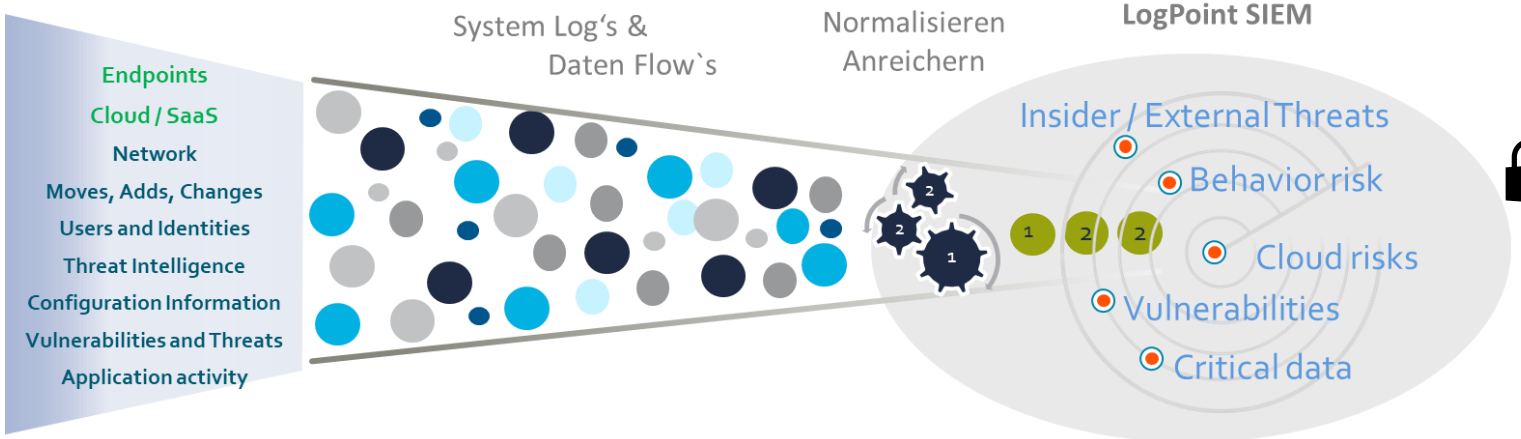


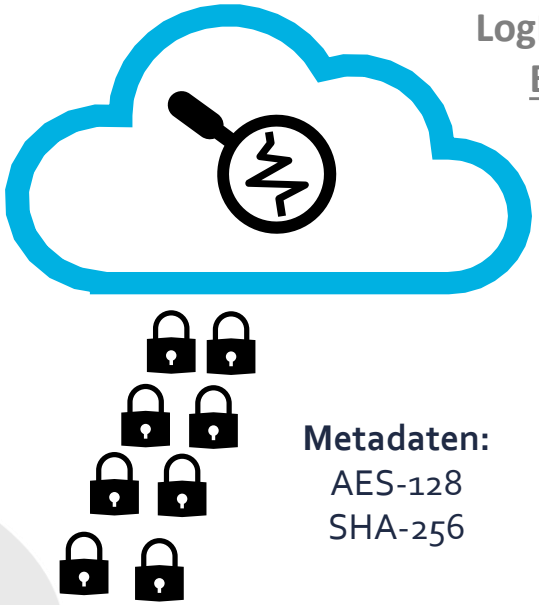
- ➢ Häufig werden Endpoints, IoT und OT Geräte aus Kostengründen nicht „beschützt“
- ➢ Jedes GB/EPS kostet zusätzlich – Kosten schlecht planbar – Datenvolumen/EPS unbekannt

- ✓ Nicht so bei LogPoint – Lightnode (Clients) kosten 1/10 eines Fullnode (FW, Server)
- ✓ SIEM Lizenzkosten exakt planbar – Fullnode oder Lightnode – egal wieviel EPS oder GB

*Security Information- und Event-Management / User and Entity Behavior Analytics

UEBA wacht inner-/außerhalb der Perimeter - Security





LogPoint UEBA
EU-Cloud

Metadaten:
AES-128
SHA-256

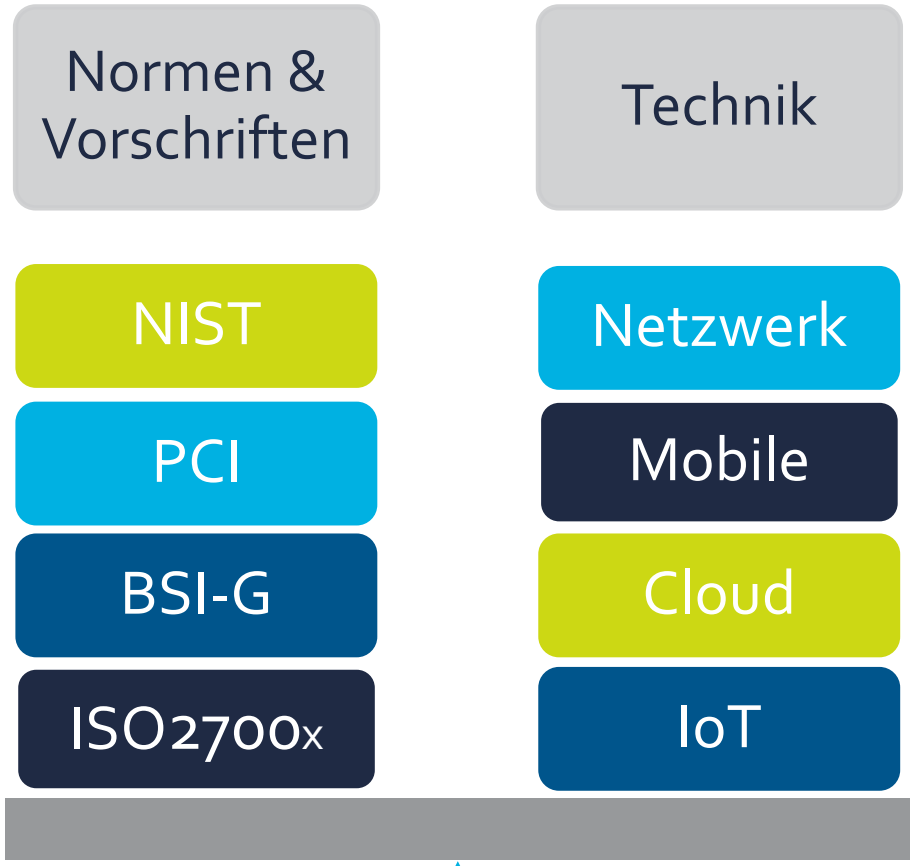
- Symmetrisch Verschlüsselt
- Key liegt beim Kunden
- Beispiel: Klaus wird zu YXcvFa
- YXcvFa wird analysiert
- YXcvFa zurück auf SIEM = Klaus

✓ UEBA Lizenzkosten exakt planbar – je Entity

Tech Data
Advanced Solutions

Sind Sie Secure wenn Sie Compliant sind?

Normen und Technik in Einklang bringen



Eine Sicherheitsarchitektur muss Normen mit Technik vereinen und den operativen Betrieb entlasten.

TechData Advanced Solutions

Aktuelle Lage

Was wollen Unternehmen?

Compliance

VS

Was brauchen Unternehmen?

Compliance & Sicherheit

1&1

Telekomunikationskonzern

Verstoß gegen DSGVO

Bußgeld: 9,55 Millionen Euro*

Der Telekommunikationskonzern habe die Daten seiner Kunden im Rahmen der **telefonischen Kundenbetreuung** zu leichtfertig herausgegeben

*Quelle: Netzpolitik.org, 09.12.2019, Ingo Dachwitz

Marriott HOTELS · RESORTS · SUITES

Hotelkette

Verstoß gegen DSGVO

Bußgeld: 110 Millionen Euro

Haben persönlichen Daten von bis zu einer 500 Mio. Gästen **Hackern** preisgegeben

*Quelle: Heise.de, 07.2019

BRITISH AIRWAYS

Fluggesellschaft

Verstoß gegen DSGVO

Bußgeld: 205 Millionen Euro

500.000 Kunden wurden bei der Online-Flugbuchung auf eine **Betrugswebsite** umgeleitet, wo ihre Daten abgegriffen wurden

*Quelle:. Informatik-aktuell.de, 30.11.2019

Prozessleitfäden und Frameworks sollen Security etablieren, verbessern und den IT-Betrieb entlasten

ISO 27001 / ISO 27002
Informationssicherheit Management

spezifiziert die Anforderungen für ein **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS)

Risikoorientierter Ansatz

DSGVO
Datenschutz-Grundverordnung

Die DSGVO ist eine Verordnung der EU, mit der die Regeln zur Verarbeitung personenbezogener EU-weit vereinheitlicht werden.

Schutz personenbezogener Daten

MITRE ATT&CK
Non Profit US-Organisation

Weltweit zugängliche Wissensdatenbank die Hacker Taktiken und Techniken aufzeigt und hilft Cyberbedrohungen genau einzugrenzen

ATT&CK zur Erstellung von Bedrohungsmodellen und -methoden

TechData
Advanced Solutions

Damit man den IT-Notfallplan hoffentlich nie braucht

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Brandrisiko: 1:100 = 1%

Cyberangriff: 1:4 = 25%

* BSI - IT-Notfallkarte (bund.de)

Was kaufen Sie sich mit einem SIEM

Die Versic

Am Beste

Relev

- D

Advanced Solutions

Konkrete Nutzen der LogPoint Lösung für Sie!

11 ISO Reports von LogPoint out-of-the-box

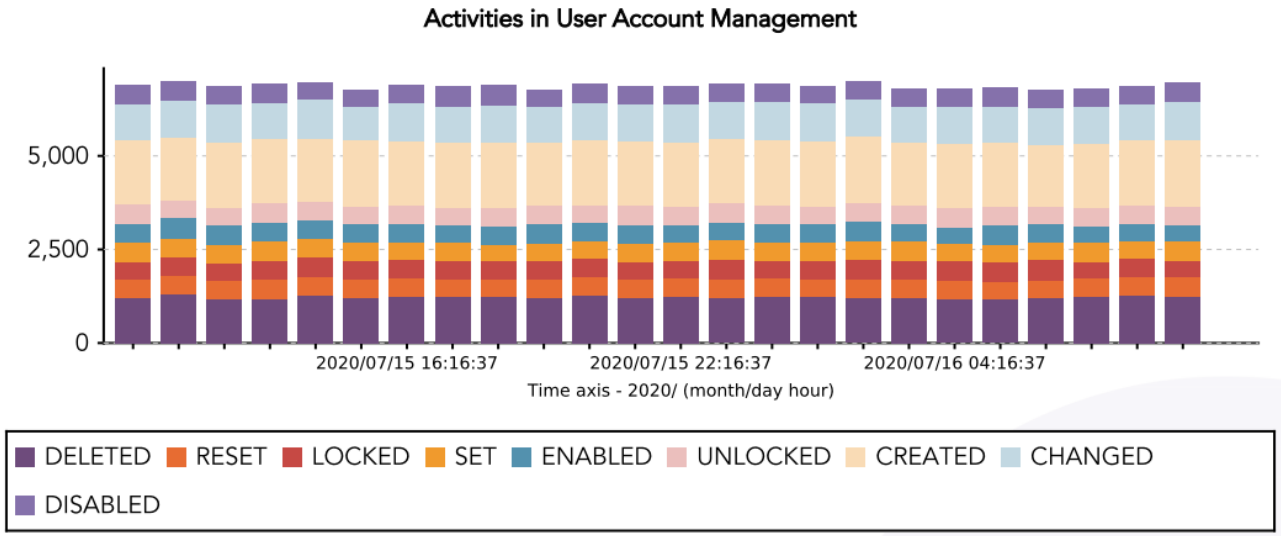
Name

- LP_ISO 27002 10_0 Communication and Operation.pdf
- LP_ISO 27002 11_0 Access Control.pdf
- LP_ISO 27002 14_0 Business Continuity Management.pdf
- LP_ISO 27002 4_0 Risk Assessment And Treatment.pdf
- LP_ISO 27002 5_0 Policy Changes.pdf
- LP_ISO 27002 7_0 Asset Management.pdf
- LP_ISO 27002 8_0 Human Resources Security (1).pdf
- LP_ISO Authentication.pdf
- LP_ISO Compliance Report.pdf
- LP_ISO Network and Connections.pdf
- LP_ISO User Account Management (1).pdf

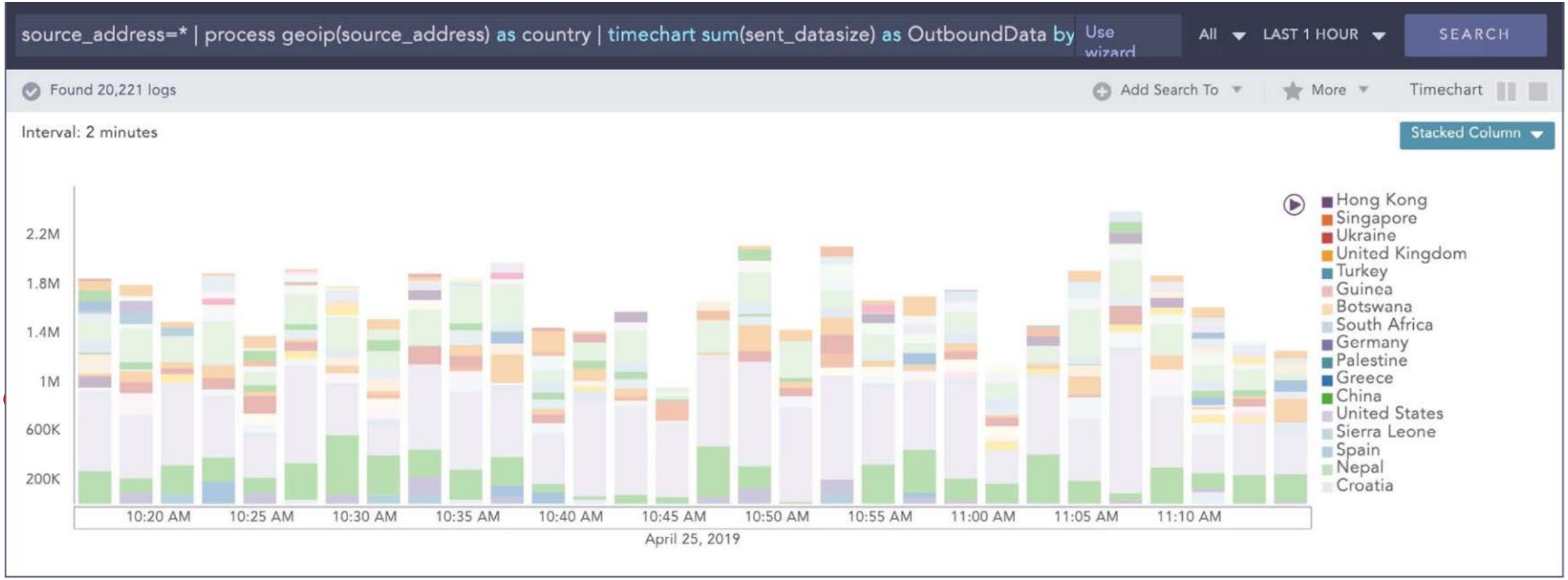
Activities in User Account Management

This chart shows the overall activities in user

This chart shows the overall activities in user account management (creation,deletion,changed etc).



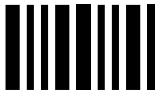
9 DSGVO Reports von LogPoint out-of-the-box



LogPoint MITRE ATT&CK Unterstützung

Herausforderung: Hacker/-Gruppe aufspüren, erkennen und abwehren

Fingerabdruck eines Hacker erkennen – **gibt es nicht!**



Code- / Angriffsmuster erkennen um auf Hacker/-Gruppe zu schließen und deren weitere Vorgehenseise zu erkennen/abzuwehren.

Problemstellung:

- Angriffsmuster muss analysiert werden
- Genutzte Tools müssen erkannt werden
- Erst die Werkzeugkombination erlaubt Rückschlüsse auf die Hacker
- Kaum SOC Analysten verfügbar und noch weniger die das wirklich können
- Begrenzte Mittel um Nachhaltigkeit zu schaffen
- Unternehmen fehlt häufig die Security Reife – „Blindflug" in Bezug auf wichtige Assests
  - Assessment?, Assetaufklärung? --- wo liegen die „Datenschätze" wirklich?
  - Hacker wissen meist besser Bescheid als eigene IT!

TechData Advanced Solutions

LogPoint MITRE ATT&CK Unterstützung

LOGPOINT

LogPoint MITRE ATT&CK Coverage

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Valid Accounts	Windows Management Instrumentation	Account Manipulation	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Exploitation for Credential Access	Network Service Scanning	Remote Services	Data from Network Shared Drive	Proxy	Exfiltration Over Alternative Protocol	Network Denial of Service
External Remote Services	Scheduled Task/Job	Valid Accounts	Valid Accounts	Valid Accounts	Brute Force	Network Share Discovery	Exploitation of Remote Services	Data Staged	Application Layer Protocol	Exfiltration Over Physical Medium	Endpoint Denial of Service
Trusted Relationship	Command and Scripting Interpreter	External Remote Services	Group Policy Modification	Masquerading	OS Credential Dumping	File and Directory Discovery	Internal Spearphishing	Email Collection	Web Service	Exfiltration Over C2 Channel	Account Access Removal
Exploit Public-Facing Application	User Execution	Scheduled Task/Job	Process Injection	Modify Registry	Forced Authentication	Account Discovery	Replication Through Removable Media	Data from Information Repositories	Ingress Tool Transfer	Automated Exfiltration	Data Destruction
Hardware Additions	Exploitation for Client Execution	Create Account	Scheduled Task/Job	Indicator Removal on Host	Network Sniffing	Query Registry	Distributed Component Object Model	Automated Collection	Traffic Signaling	Exfiltration Over Other Network Medium	Data Encrypted for Impact
Drive-by Compromise	At (Windows)	Traffic Signaling	Access Token Manipulation	Group Policy Modification	Input Capture	Remote System Discovery	Lateral Tool Transfer	Clipboard Data	Remote Access Software	Data Transfer Size Limits	Inhibit System Recovery
Replication Through Removable Media	Component Object Model	BITS Jobs	Boot or Logon Initialization Scripts	Process Injection	Cached Domain Credentials	System Owner/User Discovery	Pass the Hash	Data from Local System	Data Obfuscation	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Service Stop
Compromise Hardware Supply Chain	Dynamic Data Exchange	Boot or Logon Initialization Scripts	Abuse Elevation Control Mechanism	Signed Binary Proxy Execution	Credential API Hooking	Permission Groups Discovery	Pass the Ticket	Audio Capture	Asymmetric Cryptography	Exfiltration Over Bluetooth	System Shutdown/Reboot
Compromise Software Dependencies and Development Tools	Inter-Process Communication	Accessibility Features	Accessibility Features	File and Directory Permissions Modification	Credential Stuffing	Network Sniffing	RDP Hijacking	Data from Removable Media	Bidirectional Communication	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Exhaustion Flood
Compromise Software Supply Chain	JavaScript/JScript	Add-ins	AppCert DLLs	Deobfuscate/Decode Files or Information	Credentials from Password Stores	System Information Discovery	Remote Desktop Protocol	Input Capture	Communication Through Removable Media	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Application or System Exploitation
Default Accounts	Malicious File	AppCert DLLs	AppInit DLLs	Traffic Signaling	Credentials from Web Browsers	System Network Connections Discovery	Remote Service Session Hijacking	Screen Capture	Data Encoding	Exfiltration over USB	Data Manipulation
Domain Accounts	Malicious Link	AppInit DLLs	Application Shimming	Indirect Command Execution	Credentials In Files	System Service Discovery	SMB/Windows Admin Shares	Archive Collected Data	Dead Drop Resolver	Exfiltration Over Web Service	Defacement

Rund 130 MITRE ATT&CK Use Cases analysieren Angriffsmuster, Werkzeuge und Werkzeugkombinationen und unterstützen das SOC Team bei seiner Aufklärungsarbeit.

TechData Advanced Solutions

https://www.logpoint.com/mitre/ *

Use Cases

Use Case Beispiele:

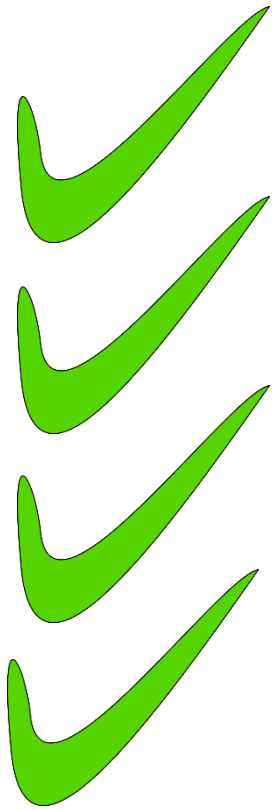
- Authentifizierungsaktivitäten. …
- Account-Management. …
- Verbindungsaktivitäten. …
- Regelbasierte Aktivitäten. …
- Bedrohung, Malware, und Schwachstellenerkennung. …
- Betriebliche Erkenntnisse. …
- Ungewöhnliches Verhalten. …
- Alarmierung und Vorfallreaktionen…

User Account Aktivierung
norm_id=WinServer label=User label=Account label=Management label=Enable -target_user=*$ -user=*$ | chart count() by log_ts, domain, user, action, target_user order by count() desc limit 10*

User Account Löschung
norm_id=WinServer label=User label=Account label=Management (label=Delete OR label=Remove) -target_user=*$ -user=*$ | chart count() by log_ts, domain, user, action, target_user order by count() desc limit 10*

Erlaubte eingehende Verbindungen basierend auf dem Standort
label=Connection label=Allow -source_address IN HOMENET source_address= destination_address IN HOMENET | process geoip(source_address) as country | chart count() by country order by count() desc limit 10*

Was erhalten Sie mit LogPoint SIEM & UEBA?



- SIEM Reports zum „ersten Kaffee“
- DSGVO-Reports Out-Of-The-Box
- ISO-Reports Out-Of-The-Box
- MITRE Support Out-Of-The-Box

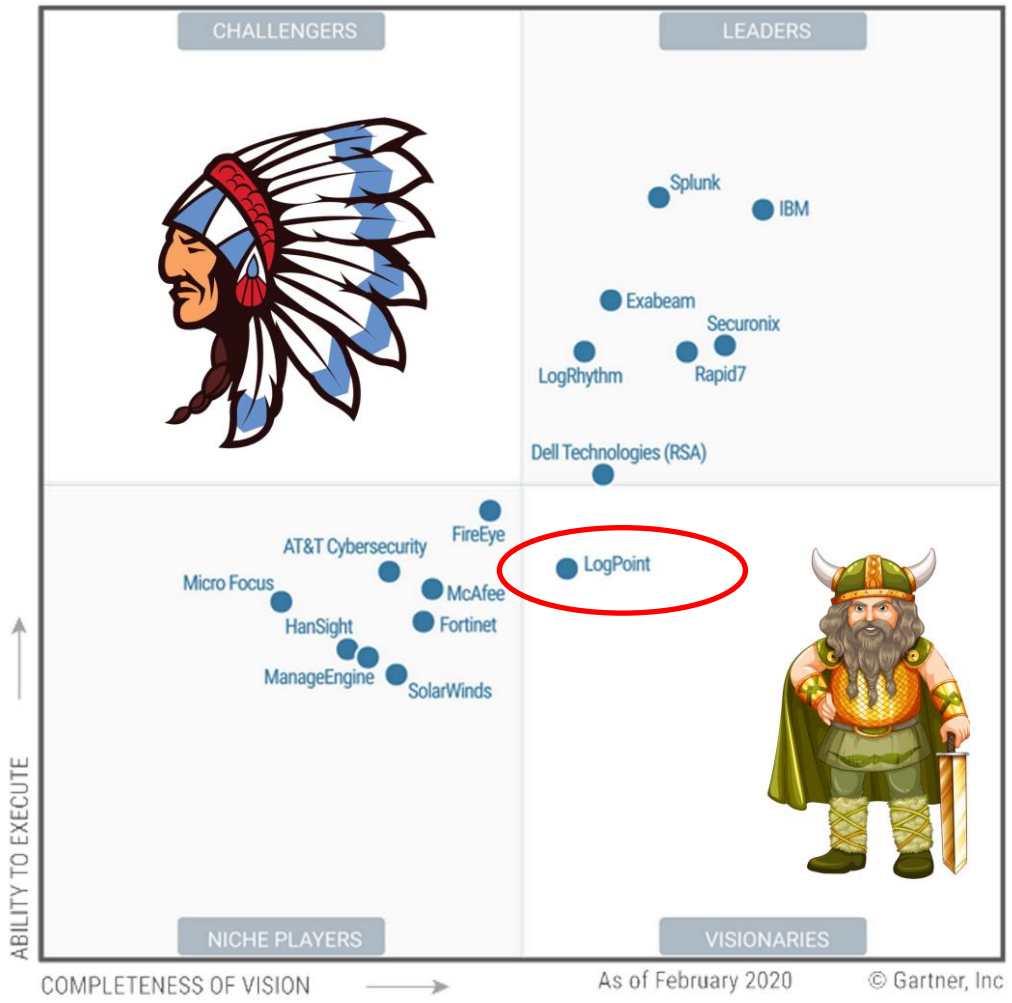
Compliance & Security

Tech Data
Advanced Solutions

LogPoint SIEM und UEBA im Überblick

Der SIEM Markt

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (February 2020)

LogPoint ist der einzige europäische SIEM Hersteller im Gartner Quadranten.

LogPoint – der Visionär

\+ Common Criteria *EAL 3+ zertifiziert, faires und einfach zu rechnendes Preismodel auf Basis von Geräteanzahl, Datenmaskierung (**data privacy mode) für DSGVO** / CCPA, gutes Cloud based UEBA, gute SOAR Integration

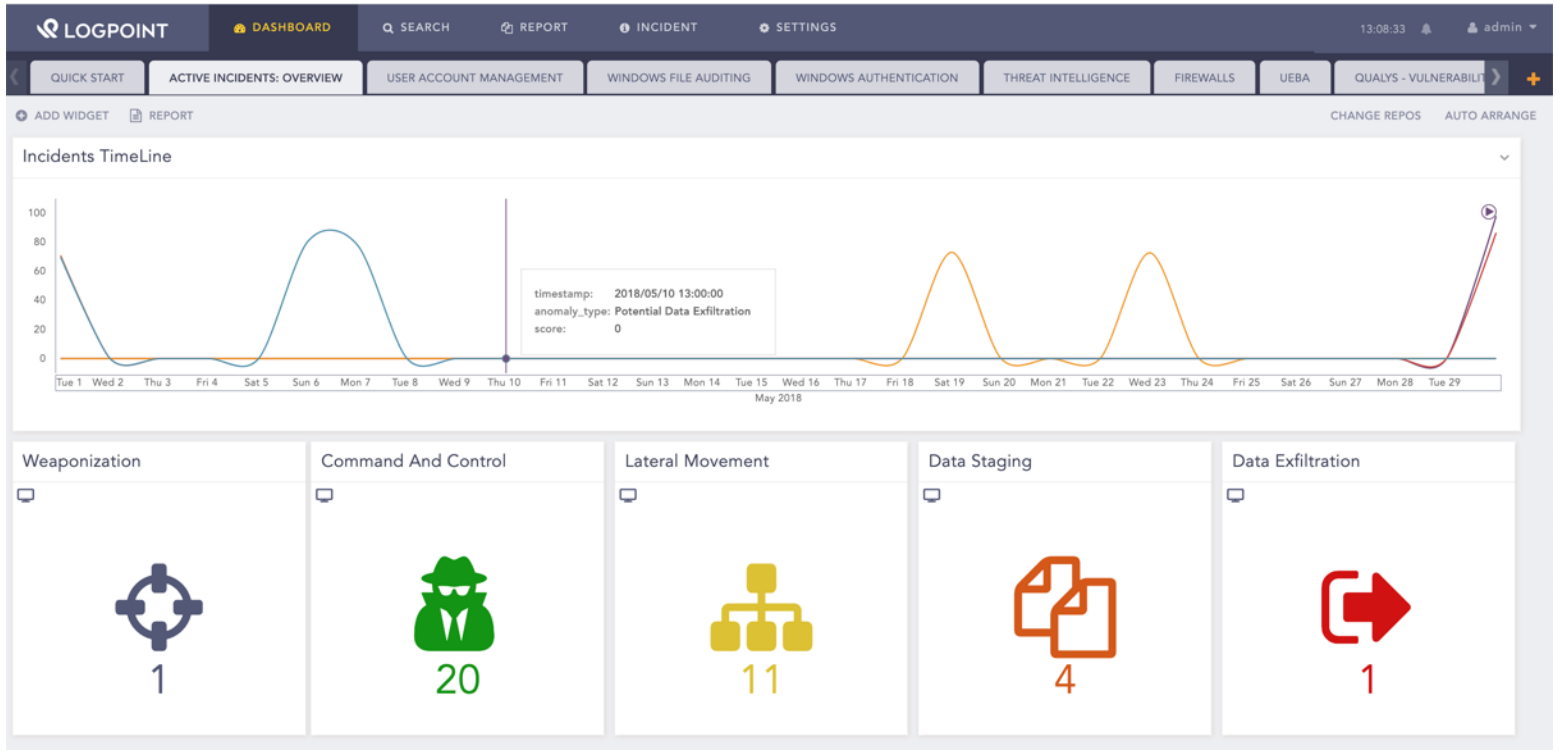
\- außerhalb Europa relativ unbekannt, keine SaaS SIEM Lösung

*EAL3+ - Version wird auf hohem Funktionsniveau „eingefroren" und mit nächst höherer Version weiter entwickelt.

Was macht LogPoint zu einem guten SIEM?

Single Source of Truth

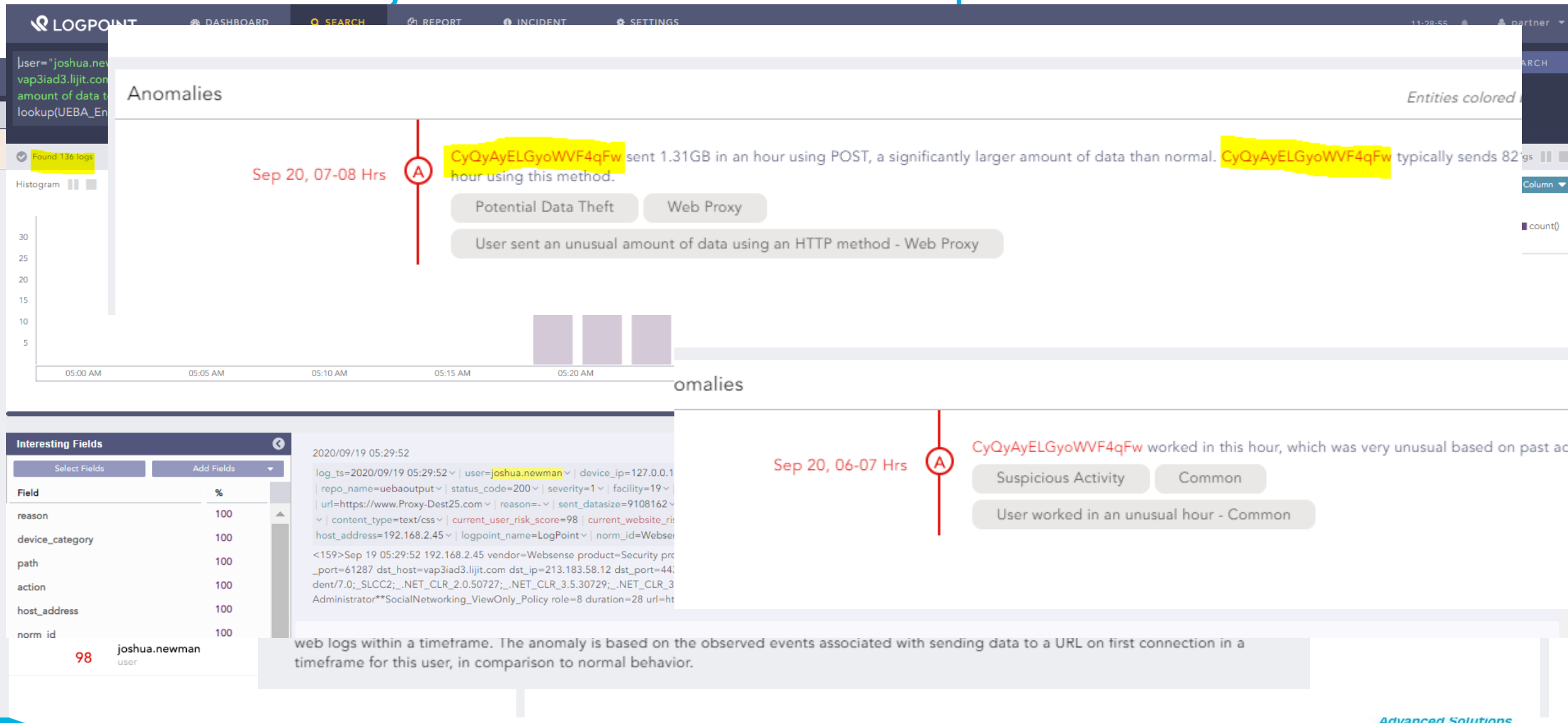
Identifizieren Sie worauf es ankommt und machen Sie es nachvollziehbar



Was ist passiert? → Wer war involviert? → Wann hat es begonnen? → Wie kam es herein? → Worauf wurde zugegriffen? → Wie wird reagiert?

TechData Advanced Solutions

Erkenntnissgewinn mit UEBA – Beispiel Datenexfiltration



Advanced Solutions

Warum LogPoint

Was hat LogPoint, was andere nicht haben?

Technik

- Unterstützung von MITRE ATT & CK-Framework
- Branchenführende Single Querry Abfrage für alle Datenquellen
- Einfaches Deployment
- Fertige Application-Packages (Log-Normalisierung)
- EAL3+ Zertifizierung

Kaufmännisch

- Exakt planbare Kosten auf Basis Anzahl der Knoten/Entitäten
- Umfassende Datenschutzfunktionen (Data Privacy Mode)
- Umfassende Compliance Reports (ISO, DSGVO, SOX, HIPPA, PCI)
- Preismodel ideal für den Mittelstand

Kunden

- Beste Bewertungen von über 1.000+ Kunden bei Service und Support
- 98% zufriedene Kunden

ata
Advanced Solutions

36

Aktuelle Lage IT Sicherheitsgesetz 2.0

Sicherheitsgesetz 2.0

Wir erwarten einen deutlichen Nachfrageanstieg in folgenden Bereichen:

1.) **SIEM und SOAR**
2.) Stringentere Umsetzung der ISO27001/2 (hohe Strafen drohen)
3.) I-OT Security rückt in den Fokus
4.) BCM = Business Continuity Management wird immer wichtiger

TechData Advanced Solutions

Vielen Dank

Wolfgang Rieger

Senior Business Development Manager DACH

Tel.: +49 (89) 4700-1128

Mobil: +49 175 7270279

E-Mail: wolfgang.rieger@techdata.com