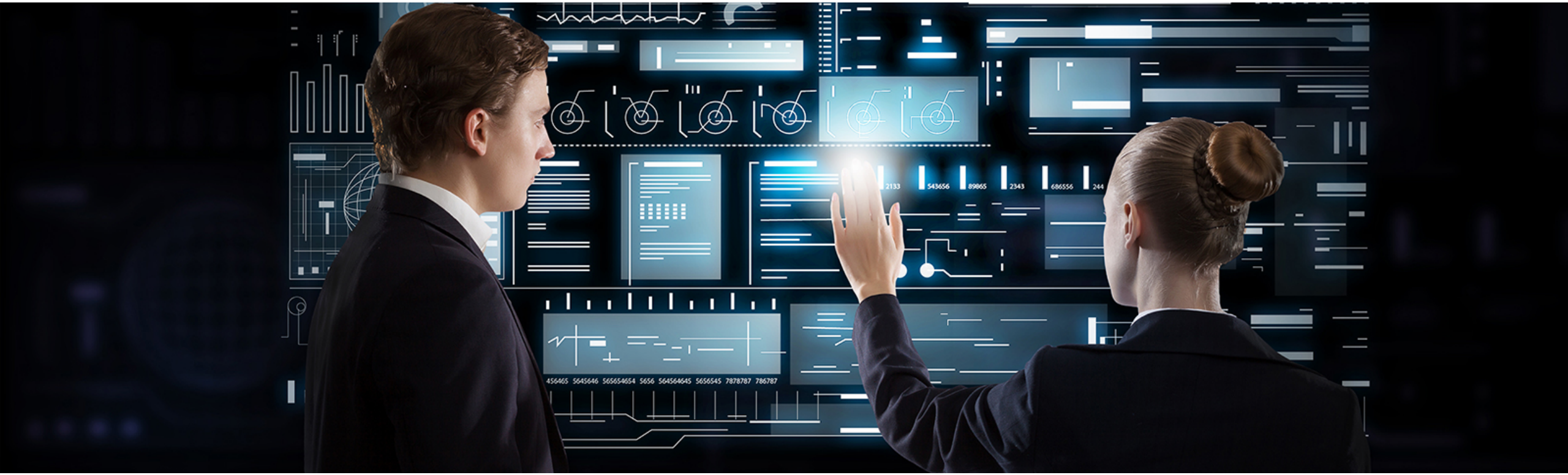
Wolfgang Rieger

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

SIEM & UEBA – lassen Sie sich informieren

was in Ihrem Netzwerk geschieht

SIEM – Security Incident & Event Management
UEBA – User Entity & Behavior Analytics



Vertrieb = CRM Kaufleute = ERP

Security = SIEM

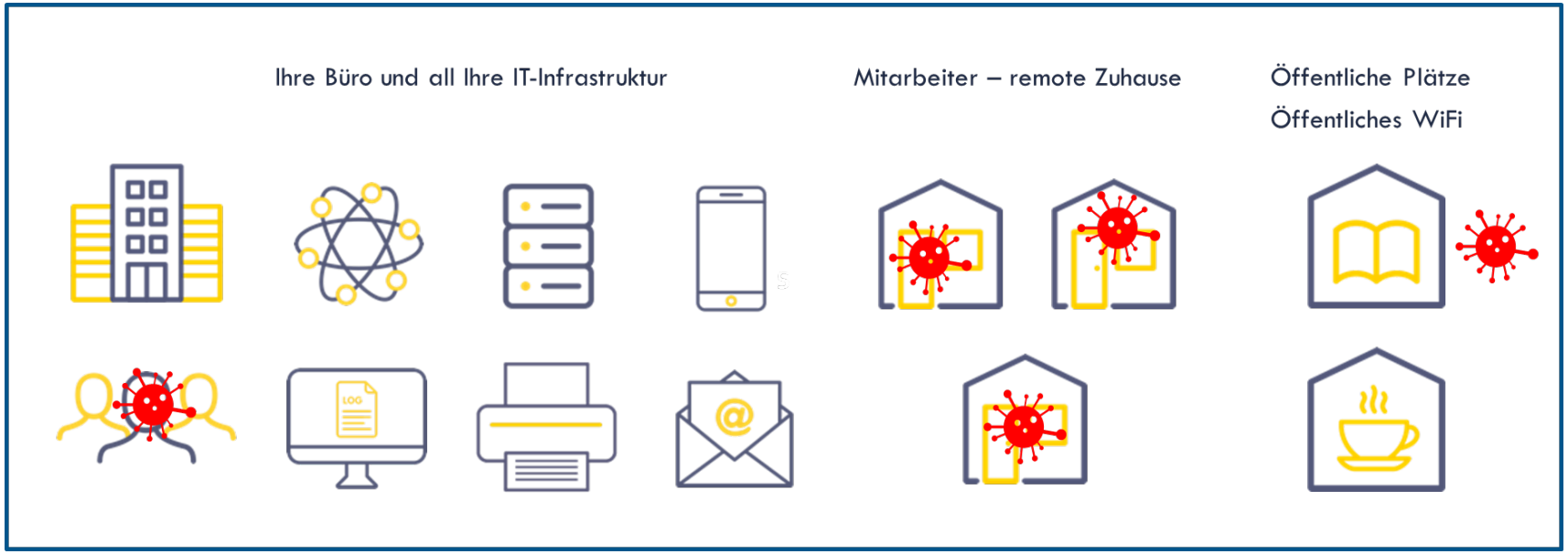
Welche Bereiche sind SIEM & UEBA relevant im Unternehmen?

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

Tech Data
Advanced Solutions

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

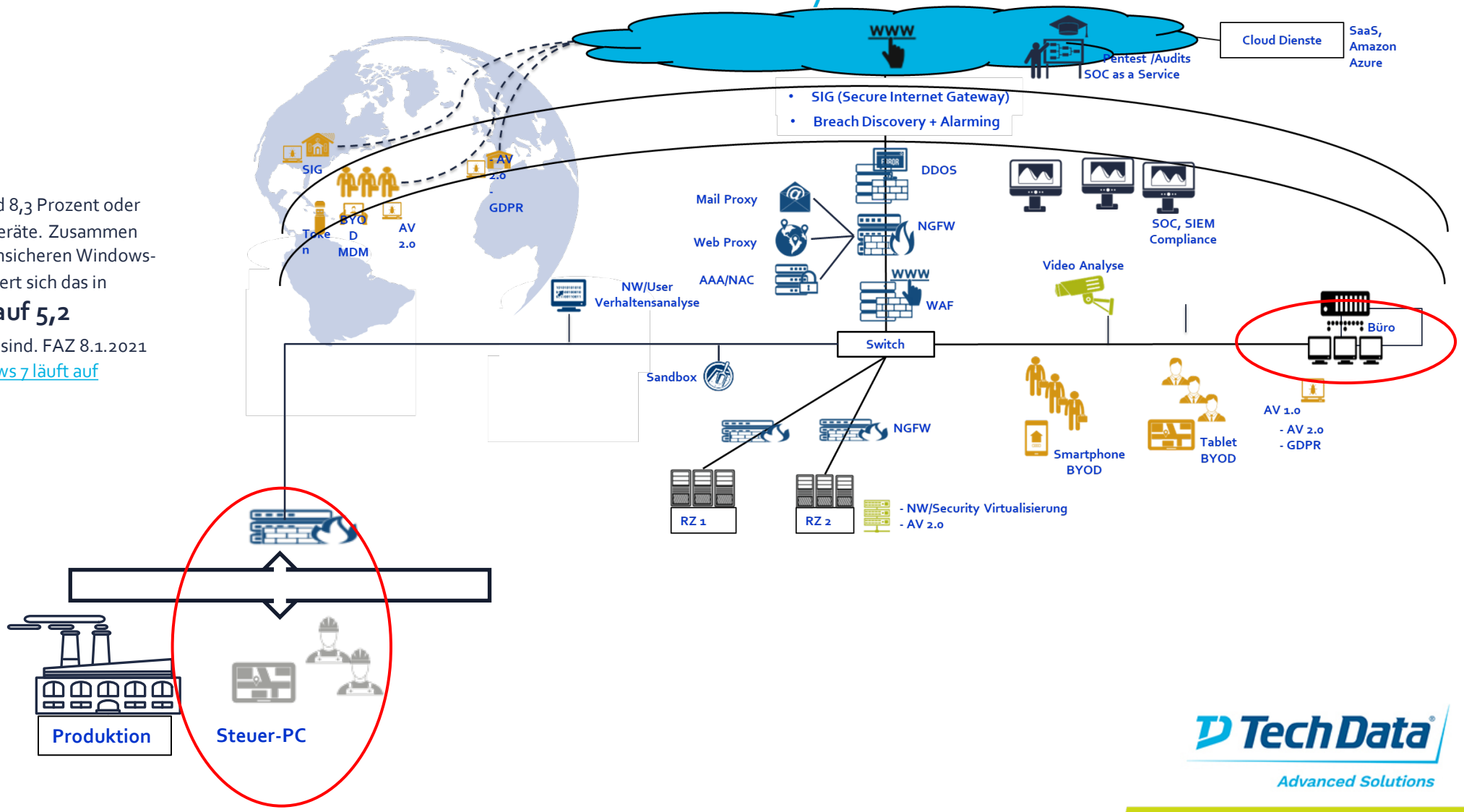
SIEM / UEBA funktionieren inner- **UND** außerhalb Ihres Netzwerkes

Tech Data Advanced Solutions

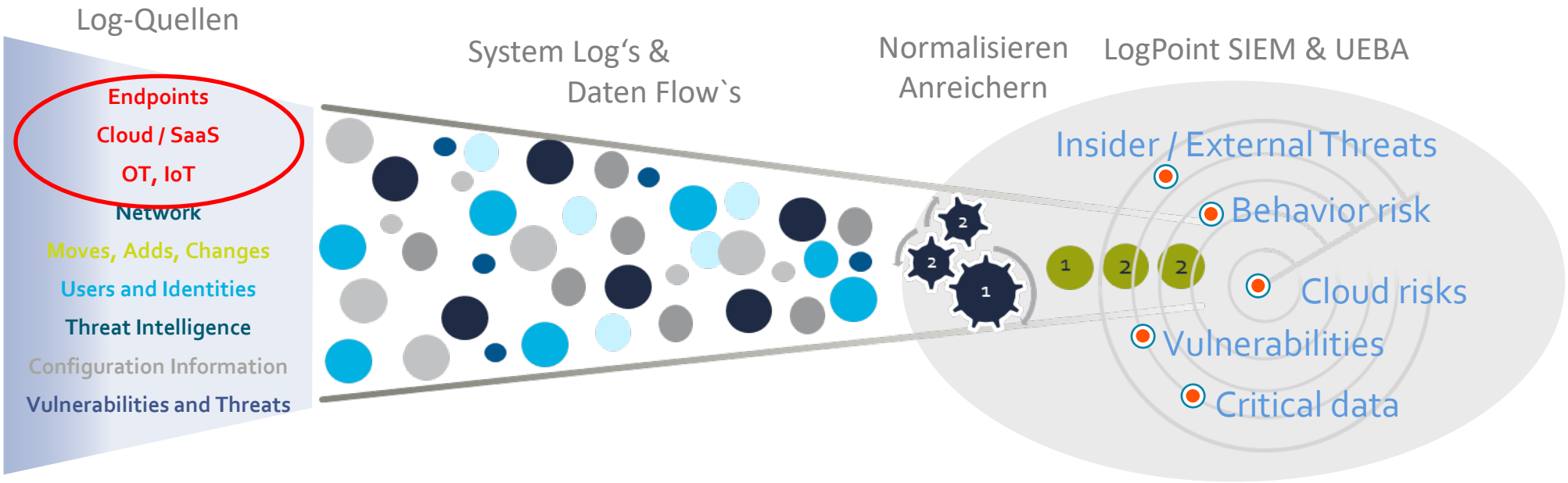
Warum gerade jetzt SIEM/UEBA so wichtig sind

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)]

Security Overview



SIEM/UEBA - Netzwerk, IoT & Industrie 4.0



- ➢ Häufig werden Endpoints, OT, IoT aus Kostengründen nicht berücksichtigt
- ➢ 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
- ✓ UEBA Lizenzkosten exakt planbar – je Entity

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

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

Tech Data
Advanced Solutions

Was kaufen Sie mit einem SIEM und weshalb?

Die Versicherung dass im kontrollierten Bereich alles ok ist!
Am Besten als **Report zum ersten Kaffee**.

Relevante Bereiche:

- Datensicherheit
- Zugriffsrechte
- Mitarbeiter
- Angriffserkennung
- Systemüberwachung
- **Compliance (ISO / DSGVO / BSI)** uvm…

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

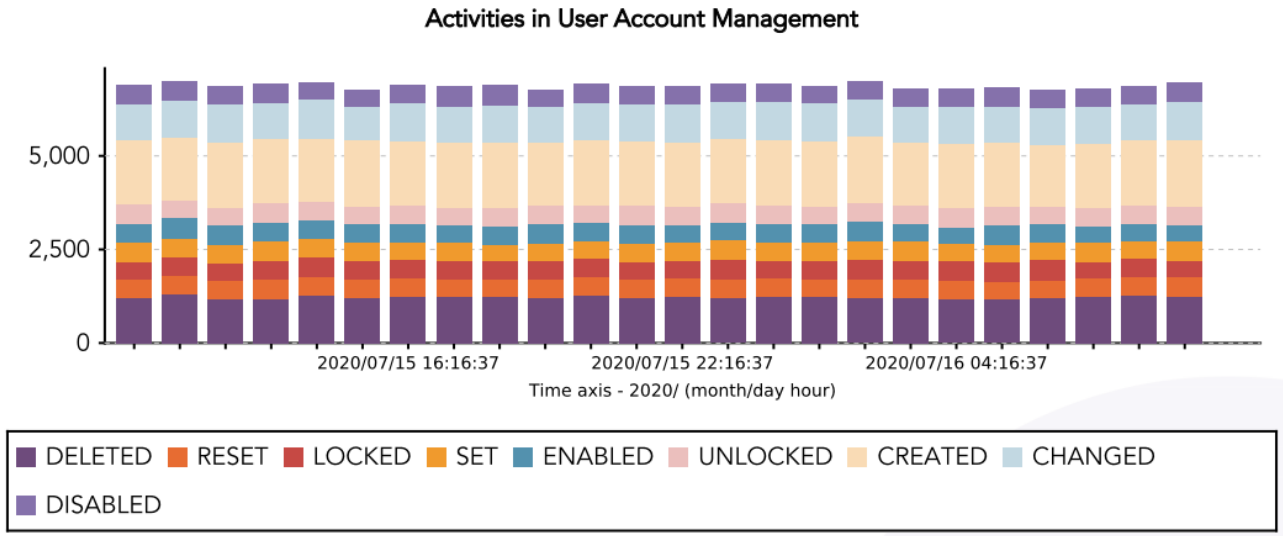
Name

- 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

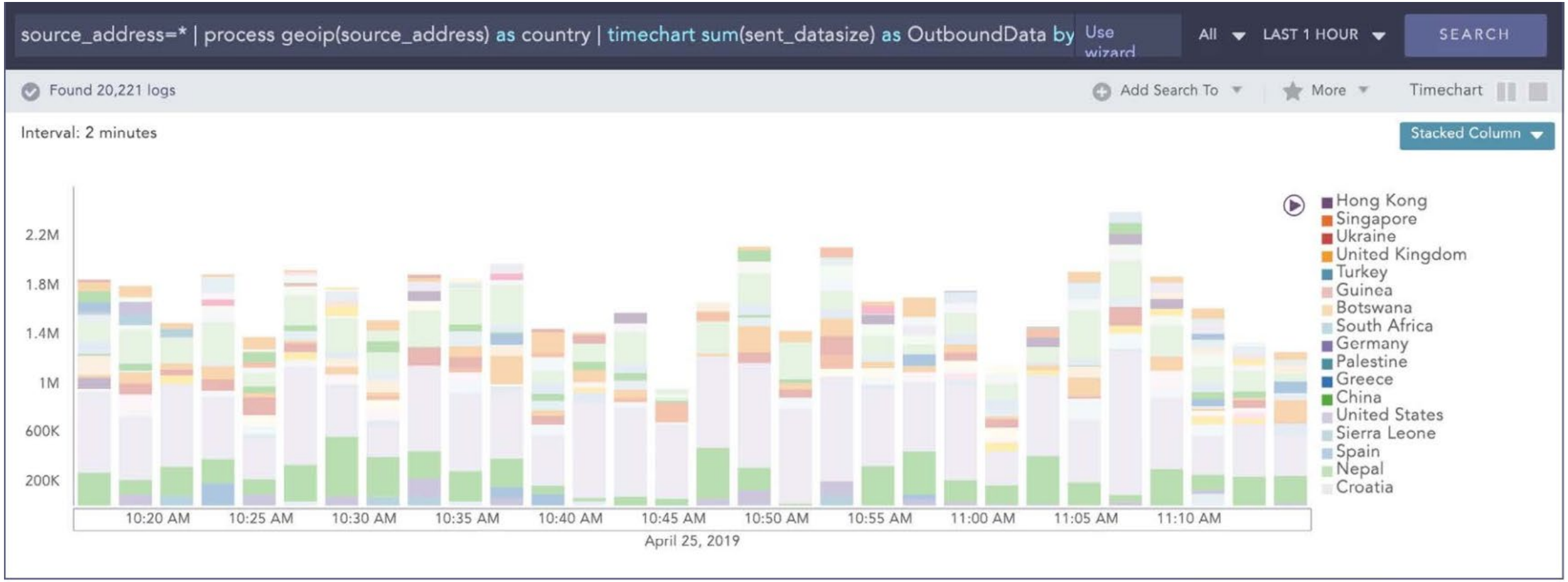
Activities in User Account Management

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

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 120 MITRE ATT&CK Funktionen analysieren out-of-the-box Angriffsmuster, Werkzeuge und Werkzeugkombinationen und Unterstützen das SOC Team bei seiner Aufklärungsarbeit

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

TechData Advanced Solutions

Erkenntnissgewinn mit UEBA – Beispiel Datenexfiltration

LOGPOINT | DASHBOARD | SEARCH | REPORT | INCIDENT | SETTINGS | 11:28:55 | partner

```
user="joshua.newman" AND request_method=CONNECT destination_host="vap3iad3.lijit.com"| process eval("user='joshua.newman'") | process eval("alert='joshua.newman sent 967.64MB in an hour to vap3iad3.lijit.com on first access, a significantly larger amount compared to what others send to new destinations.'") |process eval("threat='Potential Data Theft'")| process eval("families='User sent an unusual amount of data to a new destination - Web Proxy'")| process eval("current_user_risk_score='98'")| process eval("current_website_risk_score='90'") | process lookup(UEBA_Entity_Risk,entityName,"user,domain,destination_address,userPrincipalName","current")
```

Use wizard | All | 2020/09/19 05:00:00 TO 2020/09/19 06:00:00 | SEARCH

Found 136 logs | Add Search To | More | Logs

Histogram | Column | count()

30 25 20 15 10 5 05:00 AM

Anomalies

Entities colored

Sep 20, 07-08 Hrs (A)

CyQyAyELGyoWVF4qFw sent 1.31GB in an hour using POST, a significantly larger amount of data than normal. CyQyAyELGyoWVF4qFw typically sends 82 hour using this method.

Potential Data Theft | Web Proxy

User sent an unusual amount of data using an HTTP method - Web Proxy

Sep 20, 08-07 Hrs (A)

Suspicious Activity | Common

User worked in an unusual hour - Common

Interesting Fields

Select Fields | Add Fields

Field	%
reason	100
device_category	100
path	100
action	100
host_address	100
norm_id	100

98 joshua.newman user

log_ts=2020/09/19 05:29:52 | user=joshua.newman | device_ip=127.0.0.1 | repo_name=uebaoutput | status_code=200 | severity=1 | facility=19 | url=https://www.Proxy-Dest25.com | reason=- | sent_datasize=9108162 | content_type=text/css | current_user_risk_score=98 | current_website_ri host_address=192.168.2.45 | logpoint_name=LogPoint | norm_id=Webse

<159>Sep 19 05:29:52 192.168.2.45 vendor=Websense product=Security pr _port=61287 dst_host=vap3iad3.lijit.com dst_ip=213.183.58.12 dst_port=44 dent/7.0;_SLCC2;_.NET_CLR_2.0.50727;_.NET_CLR_3.5.30729;_.NET_CLR_3 Administrator**SocialNetworking_ViewOnly_Policy role=8 duration=28 url=ht

web logs within a timeframe. The anomaly is based on the observed events associated with sending data to a URL on first connection in a timeframe for this user, in comparison to normal behavior.

Advanced Solutions

Was bekommt Ihr Management 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

Was brauchen Sie?

Compliance
&
Security

Allianz für Cyber-Sicherheit
Teilnehmer

Tech Data
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