Cyber Security

Das Rückgrat unserer Energieversorgung

SIEMENS

Vorstellung

Siemens Schweiz AG
Arbeitgeber

Cyber Security Engineer
Tätigkeiten

Kritische Infrastrukturen
Arbeitsumfeld

Suad Emrulai

MAS Cyber Security
Studium

25 Jahre
Alter

Informatiker Systemtechnik
Ausbildung

SIEMENS

Agenda

	Thema
1	Einleitung
2	Cyber Security in der Energieversorgung
3	Hochrüsten von bestehenden Anlagen
4	Zukunft und Trends

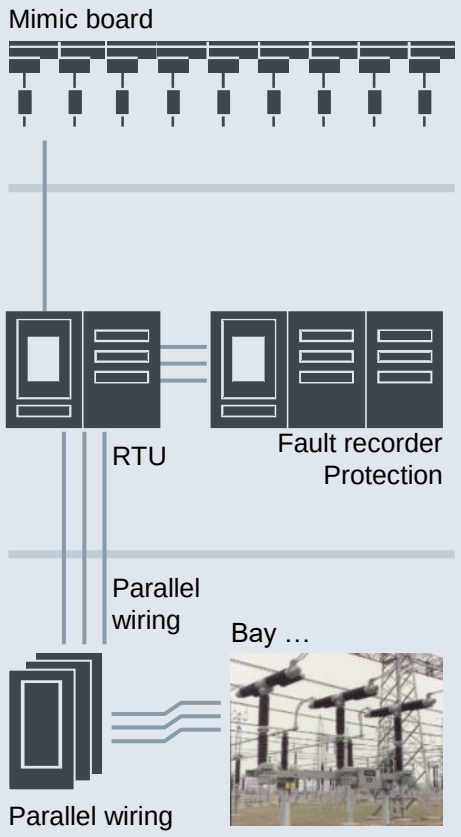
SIEMENS

Einleitung

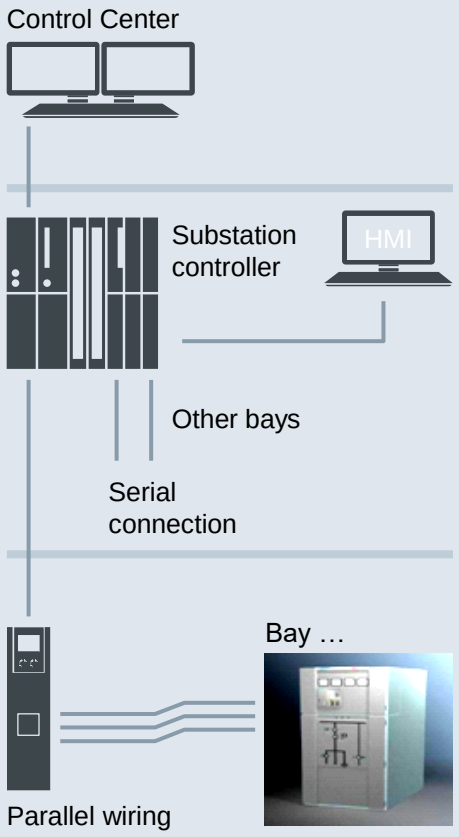
SIEMENS

Einleitung – Warum Rückgrat?

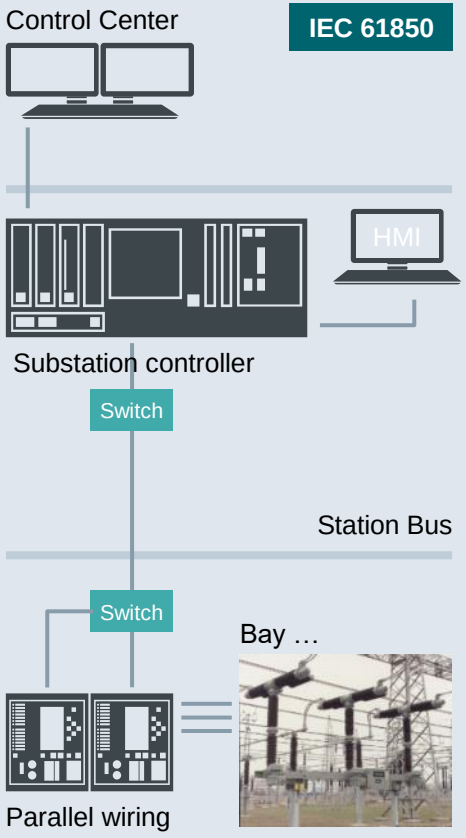
1st generation – Standard cabling



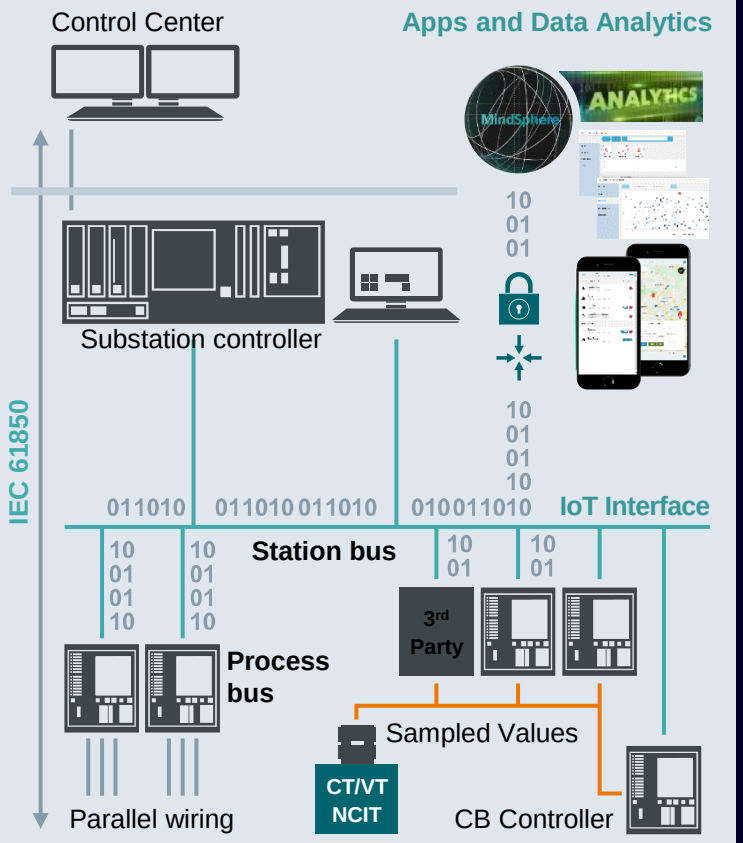
2nd generation – Point- to-point connections since 1985 …



3rd generation – Digital Station Bus since 2004 …



4th generation – Digital Grid



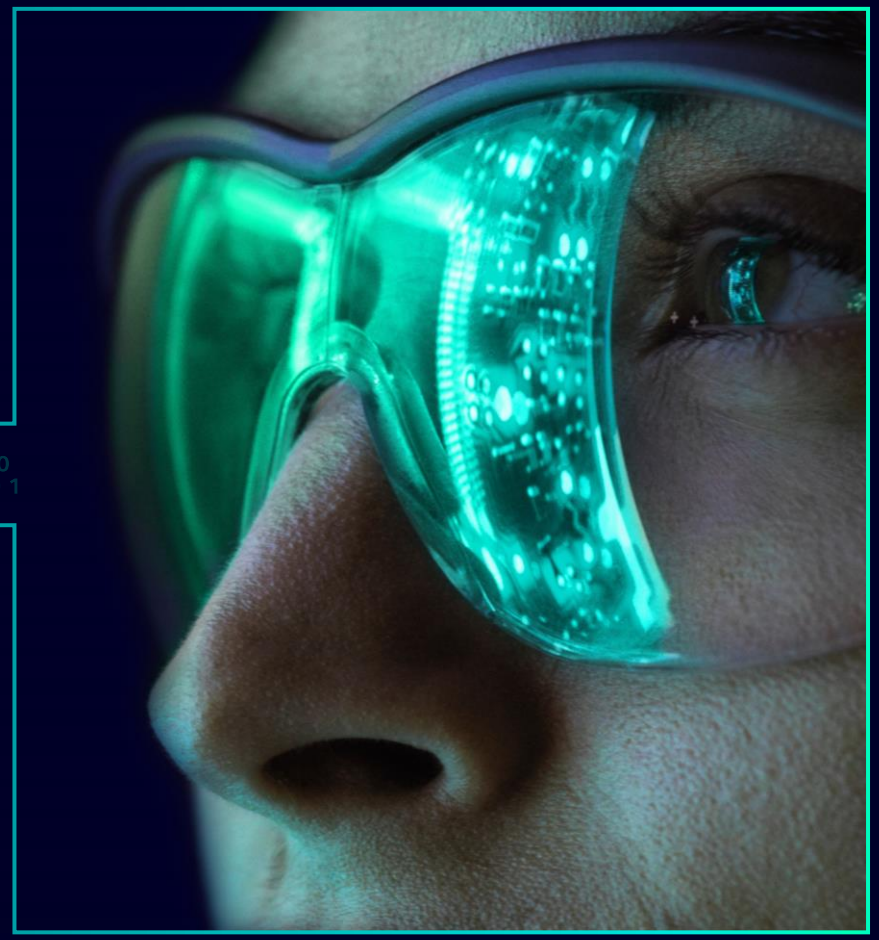
Betroffene Systeme

SIEMENS

Einleitung
Was kommt auf uns zu?

Veränderung von Infrastruktur und Prozessen

- Zunehmende Verknüpfung und Integration
- IT Standard-Komponenten
- Cloud Applikationen
- Zusammenarbeit in einem digitalen Umfeld
- Big Data und Internet of Things



- Infiltration von Malware
- D-DOS Attacken
- Menschliches Versagen, Sabotage und Spionage
- Eindringen über Fernzugriff

Veränderte Bedrohungslandschaft[1]

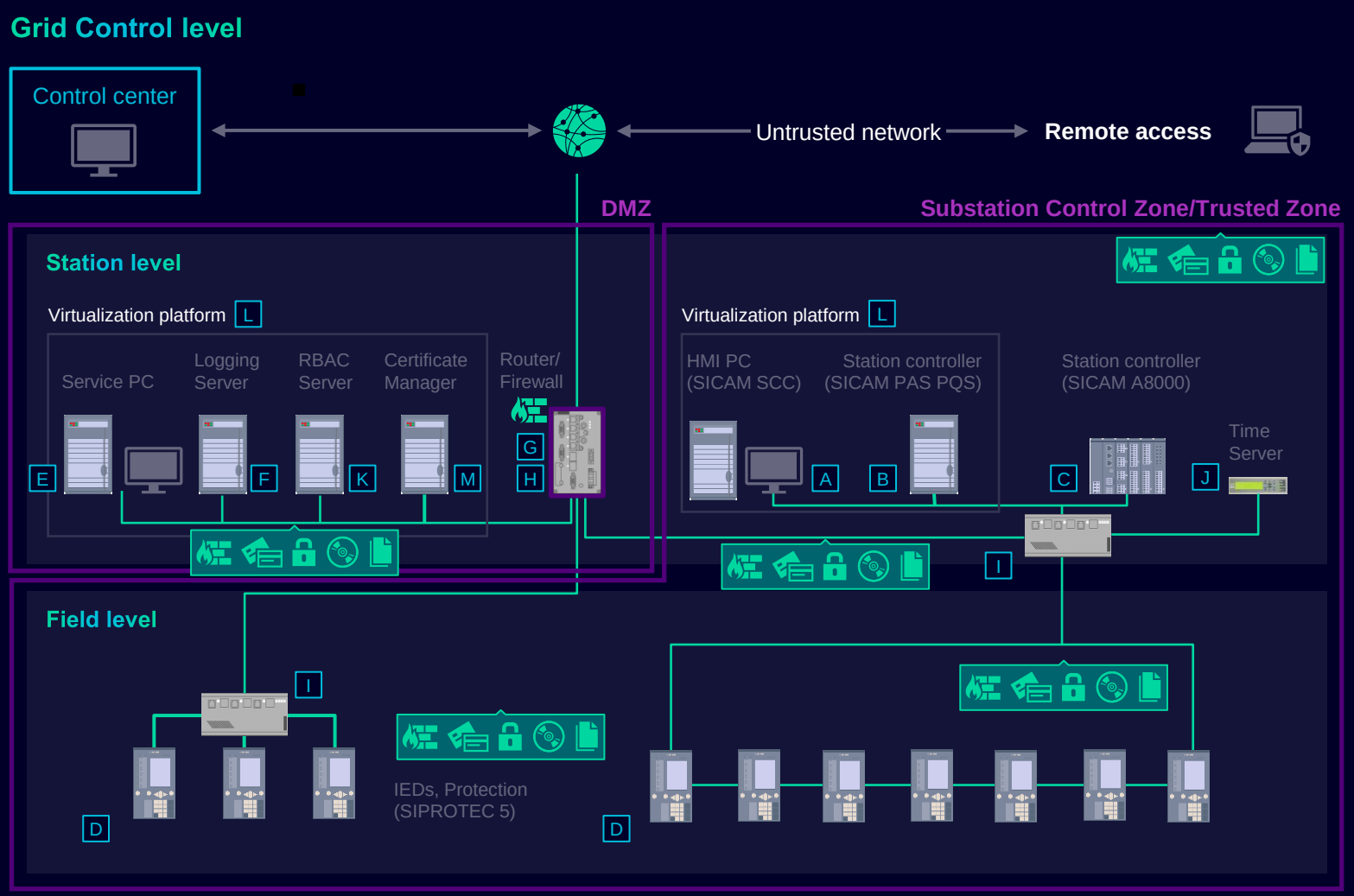
1 Based on BSI Top10 Threats 2019 for Industrial Control Systems. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf;jsessionid=15A29323F0B1EB9026255959DFD17133.internet462?blob=publicationFile&v=1

SIEMENS

Cyber Security in der Energieversorgung

SIEMENS

Cyber Security in der Energieversorgung
Absichern von Unterwerken



Massnahmen zur Cybersicherheit

- Access control and account management
- Security logging and monitoring
- System hardening
- Security patching, Backup and restore
- Malware protection
- Data protection, data integrity and system architecture
- Secure remote access

IEC 62443 certified Solution

Certified from TÜV SÜD

- IEC 62443-2-4 – Integrator processes
- IEC 62443-3-3 – Technical functionalities

SIEMENS

Cyber Security in der Energieversorgung
Personen, Prozesse, Technologie

Prozesse

Organisatorische Sicherheit & Prozesse

Personen, Richtlinien, Prozesse, Führung

Organisatorische Bereitschaft

Secure Development

Sichere Entwicklung

Umgang mit Schwachstellen und Vorfällen

Technologie

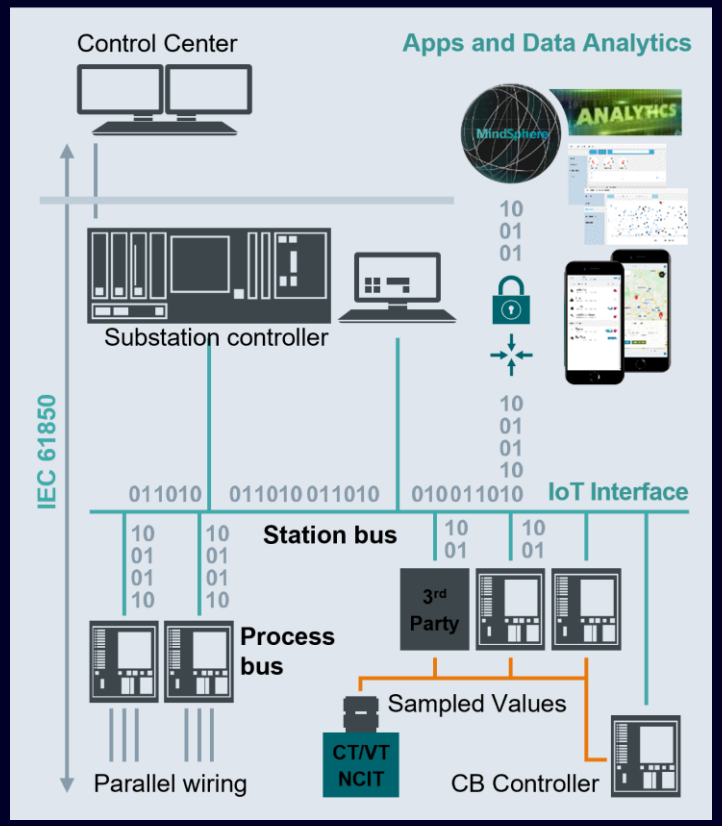
Cyber Security-Technologien, die zur allgemeinen Sicherheitsarchitektur beitragen

- Secure System Architecture
- System Hardening
- Access Control and Account Management
- Security Logging & Monitoring
- Data Protection and Integrity
- Security Patch Management
- Malware Protection
- Backup and Restore
- Secure Remote Access
- Privacy

SIEMENS

Cyber Security in der Energieversorgung
Neue Anlagen

4th generation – Digital Grid



Technologie

Cyber Security-Technologien, die zur allgemeinen Sicherheitsarchitektur beitragen

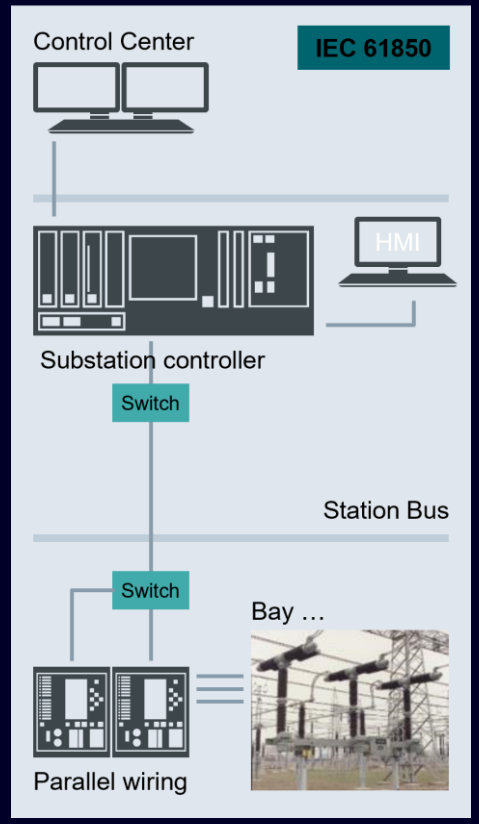
- Secure System Architecture
- System Hardening
- Access Control and Account Management
- Security Logging & Monitoring
- Data Protection and Integrity
- Security Patch Management
- Malware Protection
- Backup and Restore
- Secure Remote Access
- Privacy

Cyber Security ist bereits ein integraler Bestandteil und werden spezifisch mit geprüft

SIEMENS

Cyber Security in der Energieversorgung
Bestehende Anlagen

3rd generation – Digital Station Bus since 2004 …



Technologie

Cyber Security-Technologien, die zur allgemeinen Sicherheitsarchitektur beitragen

Secure System Architecture	System Hardening	Access Control and Account Management	Security Logging & Monitoring	Data Protection and Integrity
Security Patch Management	Malware Protection	Backup and Restore	Secure Remote Access	Privacy

Bei bestehenden Anlagen teilweise berücksichtigt oder schon vereinzelt implementiert

?

SIEMENS

Cyber Security in der Energieversorgung
Schweiz versus Europa

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE
Digital Innovation Office

Bericht vom 28 Juni 2021

Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung

Quelle: bwl.admin.ch

SIEMENS

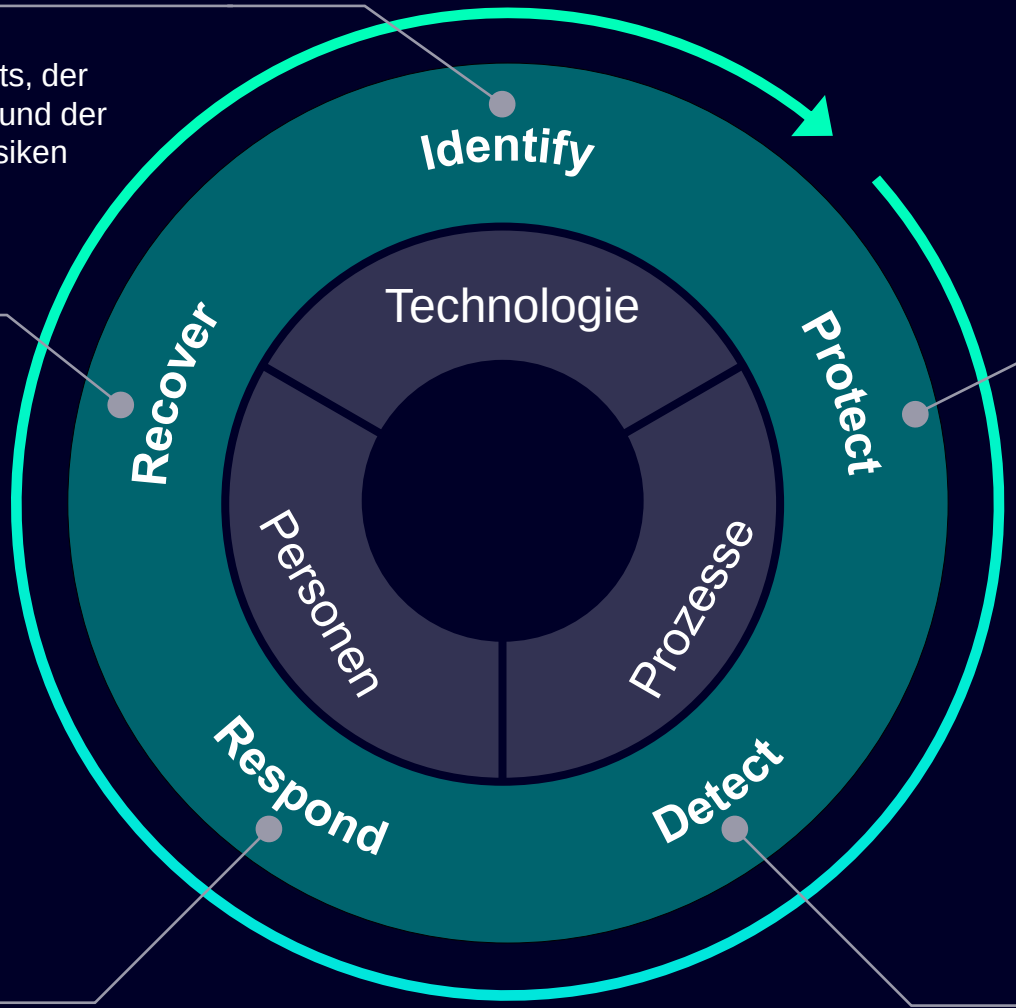
Cyber Security in der Energieversorgung
How to Cyber Security vereinfacht dargestellt

Identifizieren:

Verstehen des Geschäftskontexts, der funktionskritischen Ressourcen und der verbundenen Cyber Security-Risiken

Wiederherstellen:

Aufbau von Plänen für Betriebskontinuitätsmanagement, Wiederherstellung aller beeinträchtigten Fähigkeiten und Dienstleistungen, nach Cyber Security-relevanten Ereignissen



Schützen:

Schutz kritischer Infrastrukturen – insbesondere der Energieversorgung

Reagieren:

Gegenmassnahmen bei Cyber Security-relevanten Ereignissen

Erkennen:

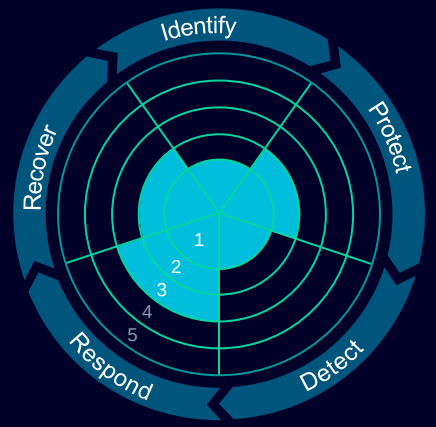
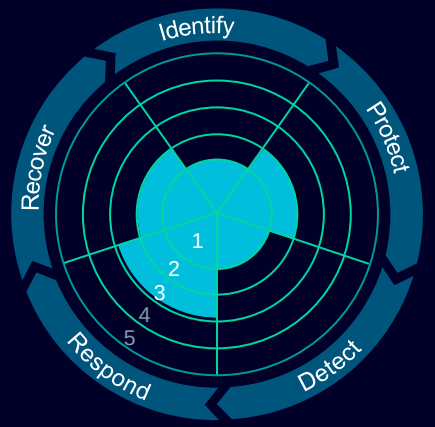
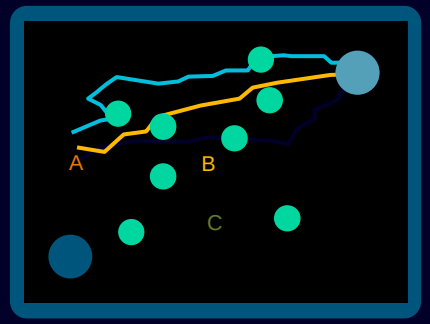
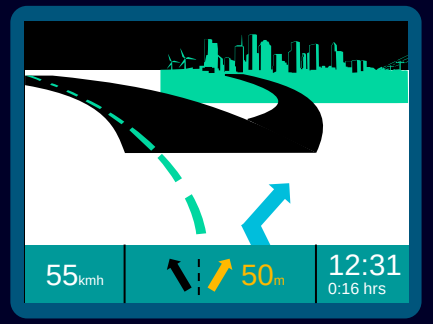
Zeitnahe Ermittlung Cyber Security-relevanter Ereignisse

SIEMENS

Hochrüsten von bestehenden Anlagen

SIEMENS

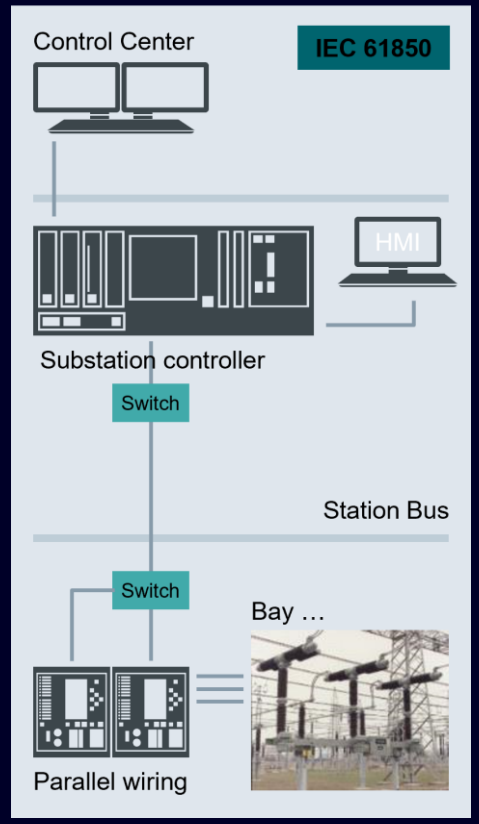
Hochrüsten von bestehenden Anlagen
Vorgehen zur Implementation von Cyber Security

	Orientierung (Ist-Analyse)	Zielbestimmung (Was ist alles umsetzbar?)	Routenwahl (Was wird umgesetzt)	Navigation (Umsetzung)
Schritte	 Status-Quo	 Status-Quo Ziel		
Was	✓ Leitsystemübersicht ✓ Netzwerkscan ✓ Schwachstellenscan ✓ Analyse Komponenten	✓ Zielbestimmung ✓ Entscheidungsgrundlagen: Priorisierung von Ressourcen ✓ Sicherheitsmassnahmen	✓ Wirtschaftlichkeitsbetrachtung ✓ Risikomanagement ✓ Variantenbildung ✓ Teil-Umsetzung	✓ Updates ✓ Hardening ✓ Virtualisierung ✓ Netzwerkscan ✓ Schwachstellenscan ✓ Dokumentation

SIEMENS

Cyber Security in der Energieversorgung
Bestehende Anlagen

3rd generation – Digital
Station Bus since 2004 …



Technologie

Cyber Security-Technologien, die zur allgemeinen Sicherheitsarchitektur beitragen

- Secure System Architecture
- System Hardening
- Access Control and Account Management
- Security Logging & Monitoring
- Data Protection and Integrity
- Security Patch Management
- Malware Protection
- Backup and Restore
- Secure Remote Access
- Privacy

- Virtualisierung
- CIS-Standard , Deaktivieren von Funktionen
- Rollenkonzept
- SYSLOG
- Richtlinien
- Updates
- Aktueller Virenschutz
- Backup / Restore Prozesse
- Netzwerkkonzept
- Passwortmanagement

SIEMENS

Cyber Security in der Energieversorgung
Lessons Learned

Folgende Punkte sind bei der Hochrüstung zu beachten:

Aktuelle und vollständige Dokumentation

Änderung der Infrastruktur → Vorbereiten

Kompatibilität prüfen

Anlage im Labor nachbilden[1]

Abnahme mit Checkliste

Inbetriebsetzung planen

Probebetrieb

[1] Typische Felder oder Teilsystem nachbilden

SIEMENS

Zukunft und Trends

SIEMENS

Zukunft und Trends

Meldepflicht bei Cyber Angriffen für kritischen Infrastrukturen

12.05.2022 - Die Vernehmlassung für die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen ist abgeschlossen. Diese hat gezeigt, dass eine Meldepflicht von Wirtschaft, Forschung und Kantonen grundsätzlich begrüsst wird. Das NCSC wertet nun alle eingegangenen Rückmeldungen aus und überarbeitet die Vorlage.

Aufgrund der zunehmenden Bedrohung durch Cybervorfälle für Wirtschaft und Bevölkerung möchte der Bundesrat das Meldewesen stärken. Die Betreiberinnen und Betreiber von kritischen Infrastrukturen sollen verpflichtet werden, dem NCSC Cyberangriffe zu melden. Damit soll eine verbesserte Übersicht über Cyberangriffe in der Schweiz ermöglicht werden. Anfang des Jahres wurden Kantonsregierungen, Betreibende von kritischen Infrastrukturen sowie Vertreter aus Forschung und Wirtschaft eingeladen, die Unterlagen zur Einführung einer Meldepflicht für Cyberangriffe zu prüfen.

Die Betreiberinnen von kritischen Infrastrukturen müssen dem **NCSC[1] Cyberangriffe nach deren Entdeckung so rasch als möglich melden**, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Gesucht sind Systeme und Lösungen die Betreiber von kritischen Infrastrukturen sowohl heutigen als auch **künftigen Anforderungen gerecht** zu werden und so ideal **beim Betrieb unterstützen**!

Quelle: https://www.ncsc.admin.ch/

[1] Nationales Zentrum für Cybersicherheit

SIEMENS

Zukunft und Trends
Sicherheitsüberwachung und Reaktion auf Zwischenfälle

Security Logging & Monitoring

Wichtigste Frage

Werde ich angegriffen?

Sicherheitsprotokollierung bedeutet, dass **alle sicherheitsrelevanten Aktivitäten im System erfasst werden**, einschliesslich Benutzerkontoaktivitäten wie An-/Abmeldung oder fehlgeschlagene Anmeldeversuche, Konfigurationsänderungen, Änderungen von Datum und Uhrzeit ...

Sicherheitsüberwachung ist die **automatisierte Auswertung aller sicherheitsrelevanten Informationen** auf der Grundlage von Regeln, die zwischen Normalbetrieb und Anomalie unterscheiden.

Operatoren werden entsprechend informiert. Bei diesen Systemen handelt es sich um Lösungen für das **Sicherheitsinformations- und Ereignis-Management (SIEM)**.

Die Zeitsynchronisation aller Netzwerkelemente ist ein MUSS, um die Nachrichten in einem SIEM korrelieren zu können:

SIEMENS

Dezentrales Logging von OT-Geräten
Beispiel: Syslog-Ereignisse Schutzgerät

8.3.2 Syslog-Ereignisse SIPROTEC 5

Schweregrad Ereignis

Die folgende Tabelle zeigt das syslog mit Schweregrad ***Ereignis***.

Ereignis	Zusätzliche Angaben	
User caused a control operation %A1%. (Benutzer hat Steuerungshandlung %A1% ausgelöst.) Zusätzliche Angaben: %A2%	%A1%	Der Typ der ausgeführten Steuerungshandlung, zum Beispiel Deaktivierung des Leistungsschalters
	%A2%	Zusätzliche Angaben zur Steuerungshandlung, zum Beispiel <FG.FN.FB.Signalname des Leistungsschalters gemäß DIGSI 5-Betriebsmeldepuffer>

Schweregrad Alarm

Die folgende Tabelle zeigt das syslog mit Schweregrad ***Alarm***.

Alarm	Zusätzliche Angaben	
While logging on to user account %A1% (%A2%-managed account) from %A3%, 3 incorrect password entries in succession were attempted. (Bei der Anmeldung an Benutzerkonto %A1% (%A2%-verwaltetes Konto) von %A3% wurde das Passwort 3-mal hintereinander falsch eingegeben.)	%A1%	Konto-ID
	%A2%	Kontotypen: • Beim produktverwalteten (lokalen) Benutzerkonto ist der Kontotyp der Produktname. • Beim RADIUS-Benutzer ist der Kontotyp ***RADIUS***.
	%A3%	%A3% kann Folgendes sein: • Der benutzerbezogene Name des Produkts, bei dem Anmeldeversuche erkannt wurden • Wenn ein Fernbedienplatz verwendet wird, ist %A3% die IP-Adresse des Fernbedienplatzes. • Bedieneinheit des Gerätes

SIPROTEC 5, Sicherheit, Handbuch
C53000-H5000-C081-4, Ausgabe 11.2020

Beispiel einer Syslog-Datei:

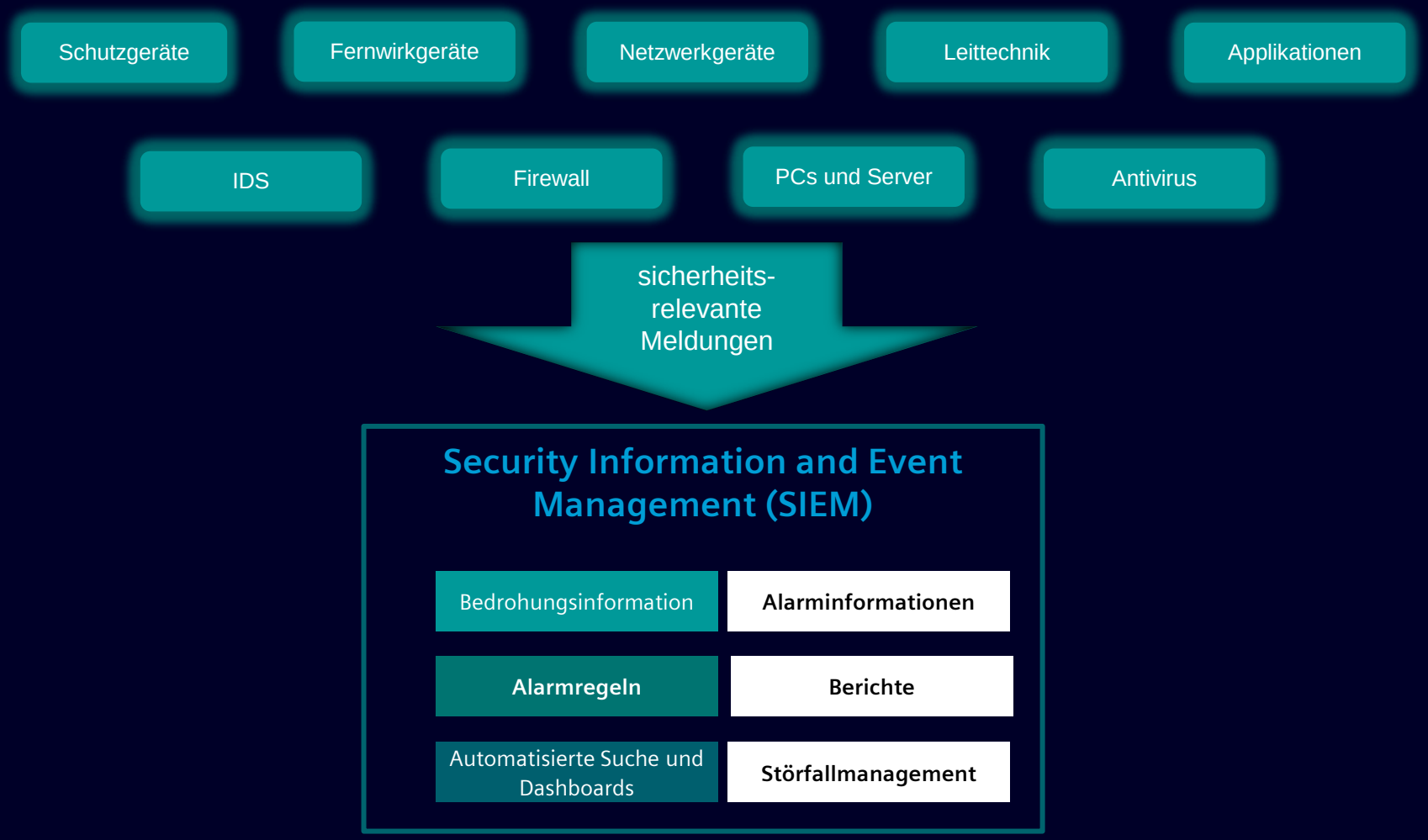
<105>1 2019-05-07T13:13:54.123+01:00 172.16.21.223 Mainboard - Siemens-Grid-Security - 'L3_TX101_7SJ82_2': Three incorrect password entries in succession were attempted while logging in to user account 'OPERATOR' ('RADIUS'-managed account) from 'HMI'.
<105>1 2019-05-07T13:13:48.246+01:00 172.16.21.222 Mainboard - Siemens-Grid-Security - 'L2_TX102_6MD85': Repeated attempt to log in to user account 'OPERATOR' ('RADIUS'-managed account) from 'HMI'.
<14>Feb 11 17:52:46 192.168.21.13 Microsoft-Windows-Security-Auditing[0x11dc]: {"EventTime":"2020-02-11T17:52:46.371858+01:00","Hostname":"SS02-HMIS01.scm.local","Keywords":"9232379236109516800","EventType":"AUDIT_SUCCESS","SeverityValue":2,"Severity":"INFO","EventID":4670,"SourceName":"Microsoft-Windows-Security-Auditing","ProviderGuid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","Version":0,"TaskValue":13570,"OpcodeValue":0,"RecordNumber":11316845,"ExecutionProcessID":4,"ExecutionThreadID":3312,"Channel":"Security","Message":"Permissions on an object were changed.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSS02-HMIS01$\r\n\tAccount Domain:\t\tSCM\r\n\tLogon ID:\t\t0x3E7\r\n\r\nObject:\r\n\tObject Server:\tSecurity\r\n\tObject Type:\tToken\r\n\tObject

Herausforderungen:

- Sammelt ein Syslog-Server die Syslog-Meldungen aller angeschlossenen Komponenten, wachsen diese Log-Files sehr schnell an.
- Diese Meldungen sind für einen Menschen eher schwer lesbar!
- Das führt dazu, dass es sehr schwer und zudem ziemlich unübersichtlich ist das regelmässig („händisch“) zu überprüfen und die wichtigen von den unwichtigen Meldungen zu trennen!

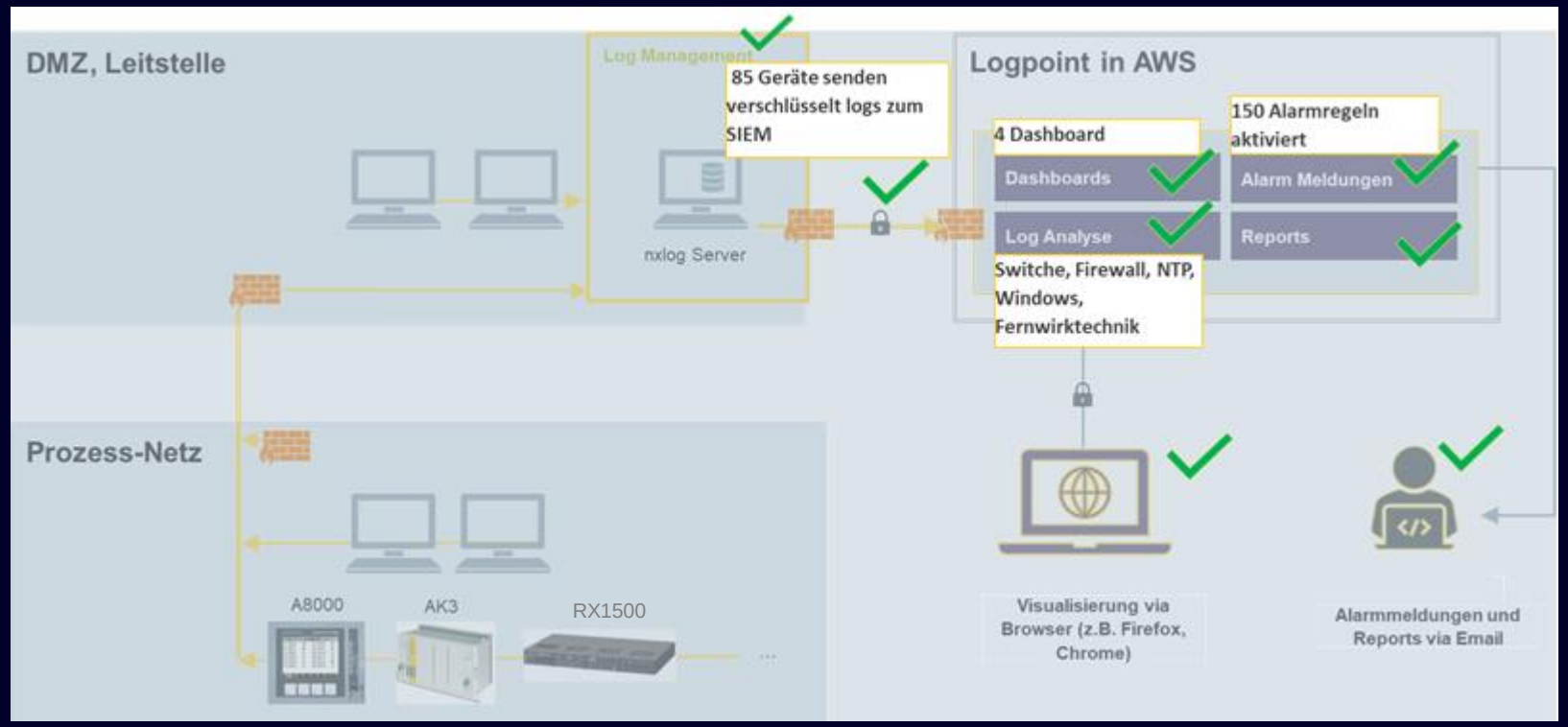
SIEMENS

Zusammenwirken von Security-Systemen und Funktionen



SIEMENS

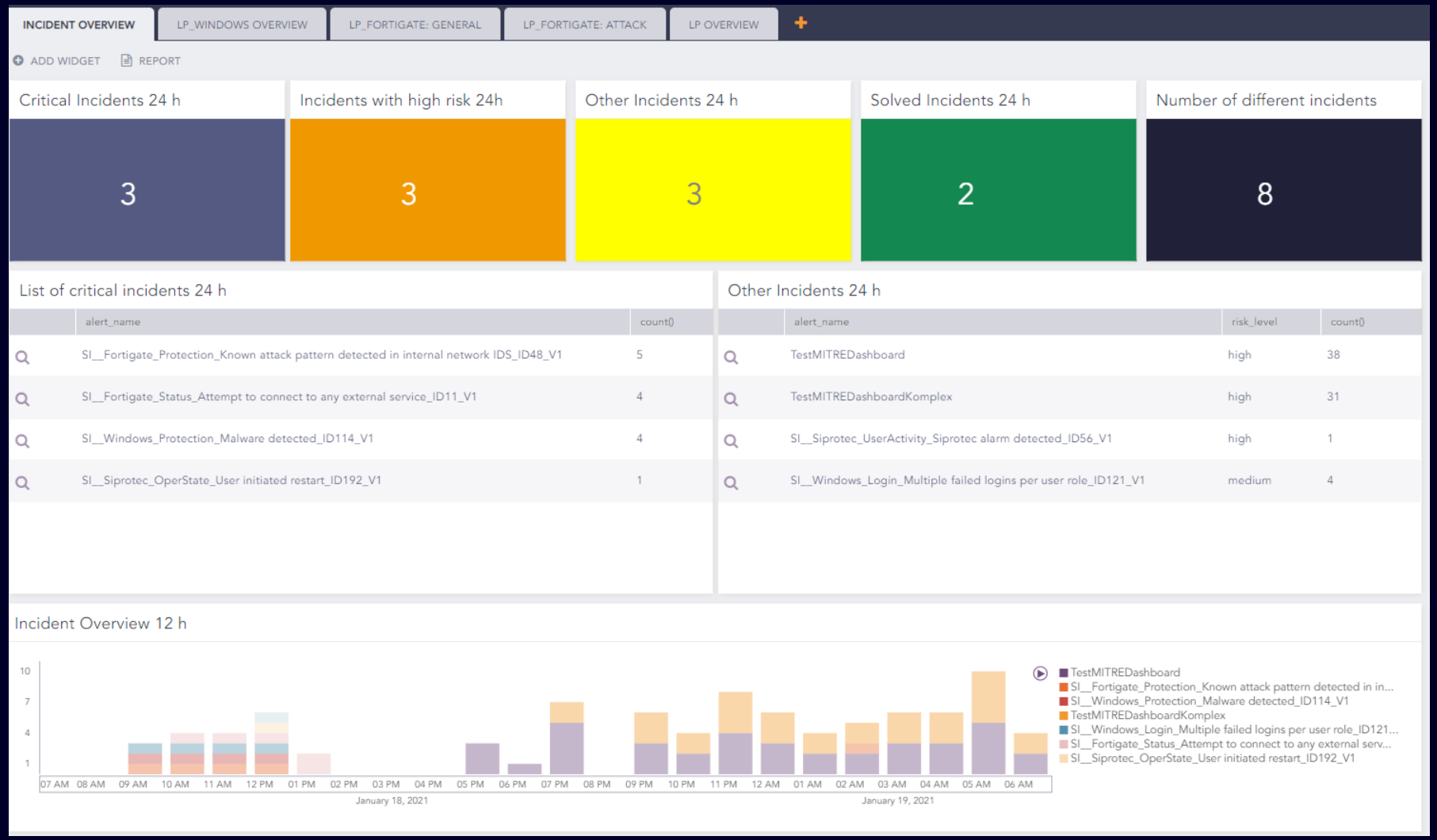
Zukunft und Trends
SIEM-System bei einem deutschen Stadtwerk



- 85 Geräte senden Logs an das SIEM-System
  - 4 Fortigate Firewalls (mit IDS)
  - 4 NTP Server
  - 26 Fernwirkgeräte
  - 20 Windows Geräte (Server, Desktop, Laptop)
  - Netzwerkkomponenten (IT) (Switche/Router)
    6 x Cisco
    14 x DigiComm
  - Netzwerkkomponenten (OT) (Switche/Router)
    10 x Ruggedcom
    1 x Westermo
- Logs von weiteren Geräten können zur Evaluierung eingebunden werden

SIEMENS

Zukunft und Trends
Alarmierung und Dashboard



SIEMENS

Zukunft und Trends
Alarmierung und Dashboard

Malware found on Testbed

[ext] Logpoint <eq-si-siem.de@siemens.com>
An EQ-SI siem

Di 17.03.2020 13:46

LOGPOINT

Alert Notification - SIE_Windows Malware detected

Message:

Event Time	Criticality	Location	Device Name	Event Source	Message	Link
2020/03/17 13:40:02	High	None	SS02_CSS	Microsoft-Windows-Windows Defender	Windows Defender Antivirus has detected malware or other potentially unwanted software.	https://go.microsoft.com/fwlink/?

Risk Level: critical
Search Link: Click Here

Event Source	Message
Microsoft-Windows-Windows Defender	Windows Defender Antivirus has detected malware or other potentially unwanted software.

SIEMENS

Suad Emrulai
Cyber Security Engineer

Siemens Schweiz AG
Freilagerstrasse 28
8047 Zürich, Schweiz
Telefon +41 585581834
Mobile +41 792298215
suad.emrulai@siemens.com
www.siemens.ch

SIEMENS