



SIEMENS
Ingenuity for life

Siemens Australia ISS

Industrial Security Services

Unrestricted © Siemens 2020

[siemens.com/industrialsecurity](https://www.siemens.com/industrialsecurity)



Building Cyber Resilience for Industry 4.0

Next-generation security in the era of digitalisation

Presenter Profile



Serge Maillet



Organisation

Siemens Australia

Job Function

**Country Segment Manager
DCP + Industrial Cybersecurity**

Years in Industry

22

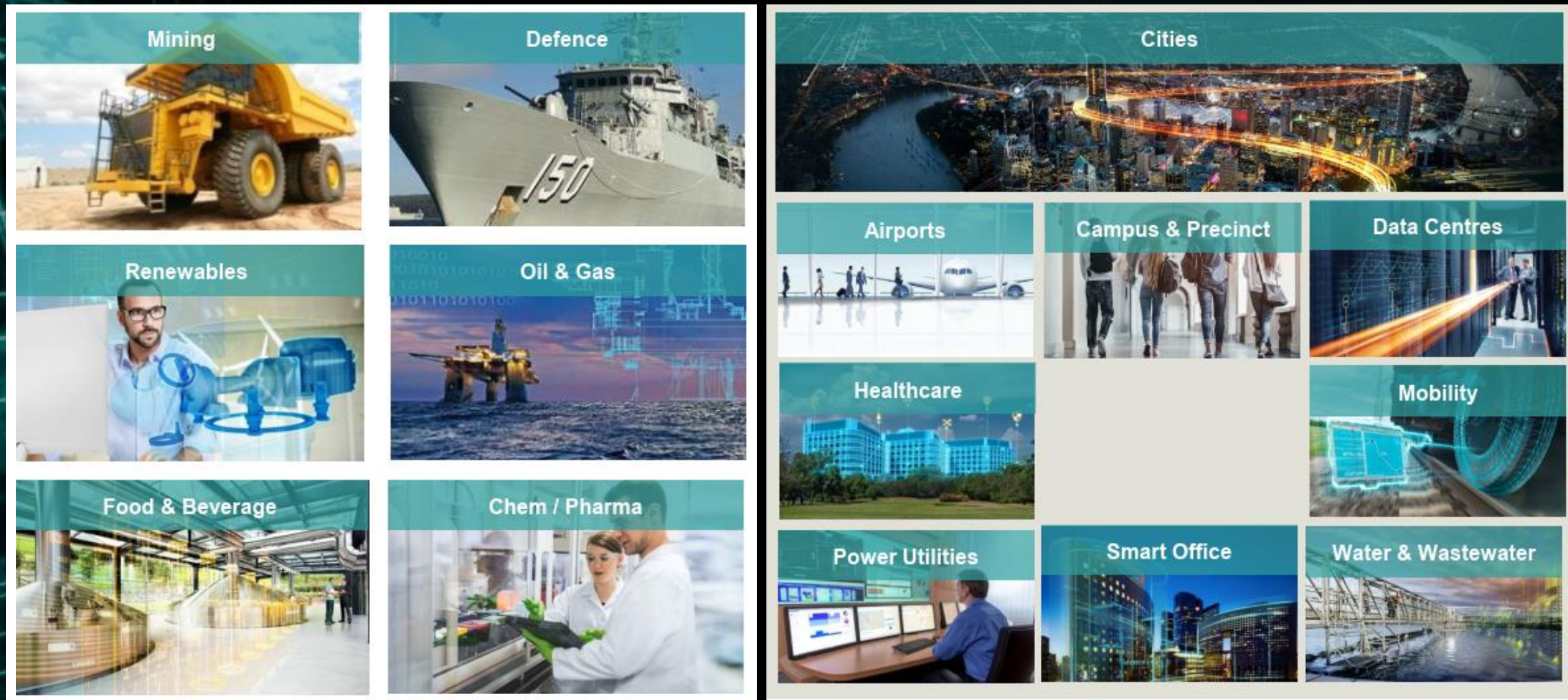
Credentials

MSc. Cybersecurity

motto: Cybersecurity is only as strong as your resilience.

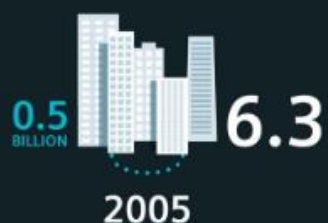
Siemens Industrial Security – key vertical market segments

SIEMENS
Ingenuity for life



By 2020, there will be
50 billion devices
connected to the internet.

Source: Cisco IBSG



Things connected to
the internet

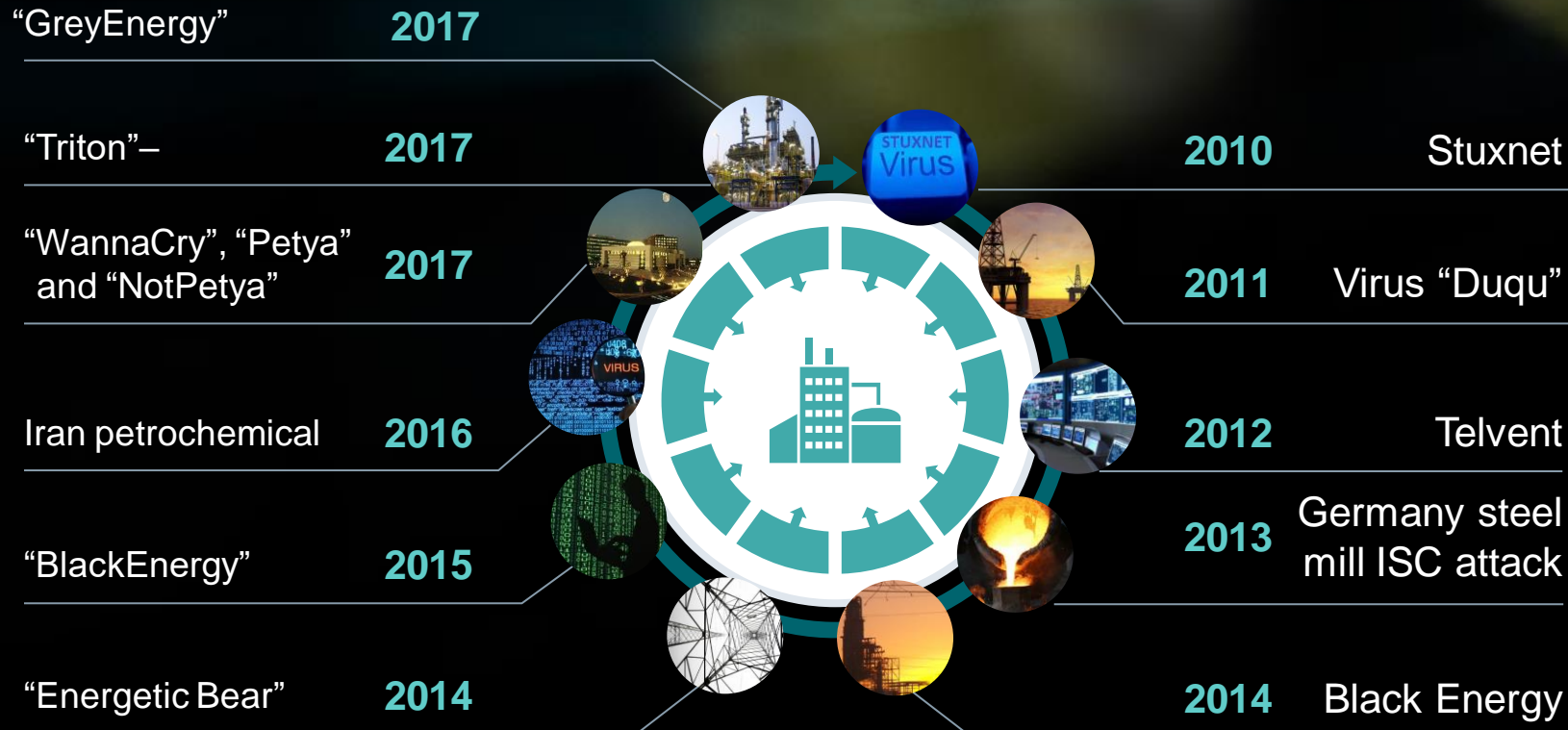


In the coming years,
40% of total data created
will be from **sensors**.

Source: Gartner



Cybersecurity attacks on critical infrastructure 2010 - 2018



Disrupting, delaying, or destroying the power supply is a big incentive

There are a variety of attackers

- Examples: Nation States, Organized Crime, Terrorist, Hacktivists

Attacks have grown in frequency and intensity

- Examples: Ransomware, Insider Threats, Phishing Attacks, Malware, Zero Day

Source: Hackmageddon, Reuters, Sans.org, NY Times, sans.org, Trend Micro, FireEye

Cybersecurity landscape in Australia



The current state of Cybersecurity for organisations in Australia: _____

Australia has recorded its largest increase of Cybersecurity events over the past 12 months compared to all other countries in APAC.

Australia currently has less than 10% of the Cybersecurity expertise that it requires to protect its industries in all industry verticals.

In 2018 – 2019, the spend on external Cybersecurity products and services in Australia reached almost AUD \$3.9 billion. The current ratio of cybersecurity services VS. products is currently 70:30.

The current potential economic cost to Cybersecurity incidents in Australia is approximately AUD \$29 billion per year (2% of GDP).

Cyber failings are now at a 'crisis' levels across most industry verticals in Australia.

Case Study: Toll Group – Ransomware Attack

Who:
Toll Group

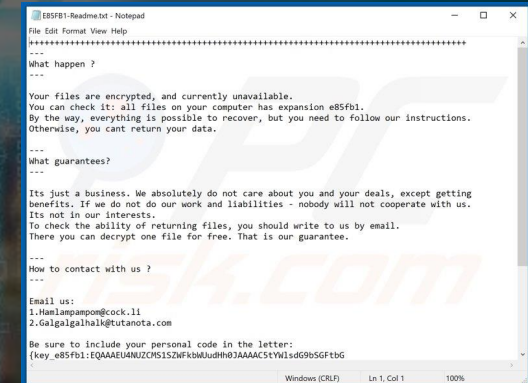
What:
Ransomware Attack on Toll's IT-OT systems
(~1000 servers infected)

Where:
Toll HQ, Melbourne - Australia

When:
31 January, 2020 (when they became aware)

How:
Mailto Ransomware (encrypted file systems)

Outcome:
Hackers demanded AUD \$8.5 million in exchange to decrypt of 5GB of data.
(it's believed that Toll decided not to pay the ransom and restore systems)



E85FB1-Readme.txt - Notepad

File Edit Format View Help

+++++

What happen ?

Your files are encrypted, and currently unavailable.
You can check it: all files on your computer has expansion e85fb1.
By the way, everything is possible to recover, but you need to follow our instructions.
Otherwise, you cant return your data.

What guarantees?

Its just a business. We absolutely do not care about you and your deals, except getting
benefits. If we do not do our work and liabilities - nobody will not cooperate with us.
Its not in our interests.
To check the ability of returning files, you should write to us by email.
There you can decrypt one file for free. That is our guarantee.

How to contact with us ?

Email us:

1.Hamlampampom@cock.li
2.Galgalgalk@tutanota.com

Be sure to include your personal code in the letter:
{key_e85fb1:EQAAAEU4NUZCMS1SZWFkbWUudHh0JAAAAC5tYWlscG9bSGFtbG

Windows (CRLF) Ln 1, Col 1 100%

Update: Toll Group attacked again in May 2020.

SIEMENS
Ingenuity for life



News / **Toll Group** resists ransom demands from hackers after ...

theloadstar.com - 12 May 2020

However internal sources do point to a **cyber attack**." Mr Jensen added that, following a webinar on **cyber security**, he came away with "the clear ...

Toll Group's corporate data stolen by attackers

iTnews - 11 May 2020



ACS

Toll Group data dumped on dark web

Posting on dark net site for corporate leaks 'onion', the cyber criminals scolded Toll for its security measures after the company's systems were ...
May 21, 2020



Toll customer data stolen in its second **cyber attack** of 2020

Inside Retail - 12 May 2020

Toll Group managing director Thomas Knudsen said the **attack** was unscrupulous, and that the business is working with the Australian **Cyber** ...

Toll Group reveals stolen data may show up on dark web

CRN Australia - 12 May 2020

Question: Should you ever pay hackers' ransom demands?

SIEMENS
Ingenuity for life

Ransomware attacks in 2019 cost Australian businesses and public-sector organisations **\$241M**

The average operational downtime organisations face following a successful ransomware attack is **16 days**

The estimated downtime costs whilst recovering from a ransomware attack **\$15,000/day** not including lost production time!

Paying ransom to hackers is almost always a bad idea and is highly discouraged in the majority of cases!

An ounce of prevention is worth a pound of cure!



Top 5 Vulnerabilities, Risks and Exposures for Industry



1. Industrial Control Systems (ICS) software applications and operating systems are outdated and vulnerable to CVEs.
2. Industrial networks are ineffectively segregated and segmented.
3. Poor system and operating system hardening and patch management.
4. Weak physical and logical access control.
5. Insufficient logging and monitoring of mission-critical systems.

The advanced persistent threats targeting industry are emerging and evolving.

Industrial Security is particularly challenging

SIEMENS
Ingenuity for life



Key components of an effective industrial security strategy



Credible

Implement fundamental security controls consistent with IT and OT Security governance and best industry practices.

Deep OT awareness for accurate risk assessment.



Efficient

Integrate into existing operational processes and orchestrated workflows.

“Low noise and high context”:
Minimum effort to achieve risk reduction.



Non-Disruptive

Avoid distracting IT and OT staff with complex tools and technology.

Create absolute minimum risk to production availability or operational safety.,

Gartner

"Implementing effective security governance in an integrated IT/OT environment is difficult because the two domains have different risk appetites and security requirements. Security and risk management leaders need a single governance structure to support both domains and balance their requirements."

Gartner, 10 October 2019, Document: G00441788

4 Simple Phases to Building Cyber Resilience



Phase 1: Preparation



Phase 2: Detection



Phase 3: Response



Phase 4: Recovery

Phase 1 --- Preparation

Determine risk profile and security posture. Create a strategy for business & operational continuity coupled with periodic security risk assessments.

Develop cyber governance policies using regulatory and industry security frameworks such as IEC 62443 and ISO 27001.

Determine which systems and subsystem assets have potential security risks, vulnerabilities and exposures. Develop patch management strategy.

Develop a Disaster Backup & Recovery Strategy (DBRS). Continuously backup critical system assets and test backup integrity.

Educate your entire staff with ongoing security awareness training. 90% of security breaches are caused by human error.

Preparation is directly proportional to the effectiveness of security.

Phase 2 --- Detection

Develop a cyber-threat awareness platform using global threat intelligence from government agencies and industry sources.

Implement active (real-time) security monitoring tools such as Network Management Systems (NMS) coupled with Continuous Threat Detection tools underpinned by Artificial Intelligence (AI) and Machine Learning (ML).


Respond to threats including suspected security breaches and attacks as early as possible to ensure the most timely response and recovery.

Ensure the integrity and preservation of information on attacks for the purpose of reconnaissance and digital forensics.

Detection requires advanced situational awareness.

Phase 3 --- Response

SIEMENS
Ingenuity for life



Establish an incident response plan with escalation procedures. Conduct response drill scenarios and conduct regular mock data breaches to evaluate roles and responsibilities in the event of a security incident.

Leverage Security Incident and Event Management (SIEMs) tools to aid in the identification, monitoring, recording and root cause analysis of security incidents and breaches.

Maintain the objective of containing a breach when it's first discovered to avoid the attack spreading to other system assets.

Determine legal implications. Avoid the destruction of valuable evidence to aid in the root cause analysis and subsequent forensic investigations.

Rapid response to minimise damages and improve recovery time.

Phase 4 --- Recovery

Document Method of Procedures (MOPs) and Playbooks for recovering your industrial system and subsystems following a security breach.

Know who to call for reporting security incidents. This includes impacted customers, governing organisations, Federal & State Government, etc.

Implement a backup and recovery system underpinned by regular backups with integrity to restore systems corrupted by an attack.

Document all elements of the security breach or attack for the subsequent analysis activities including forensics investigation.

Disaster recovery is not about IF... it's about WHEN.

Industrial Security Technologies & Best Practices

SIEMENS
Ingenuity for life

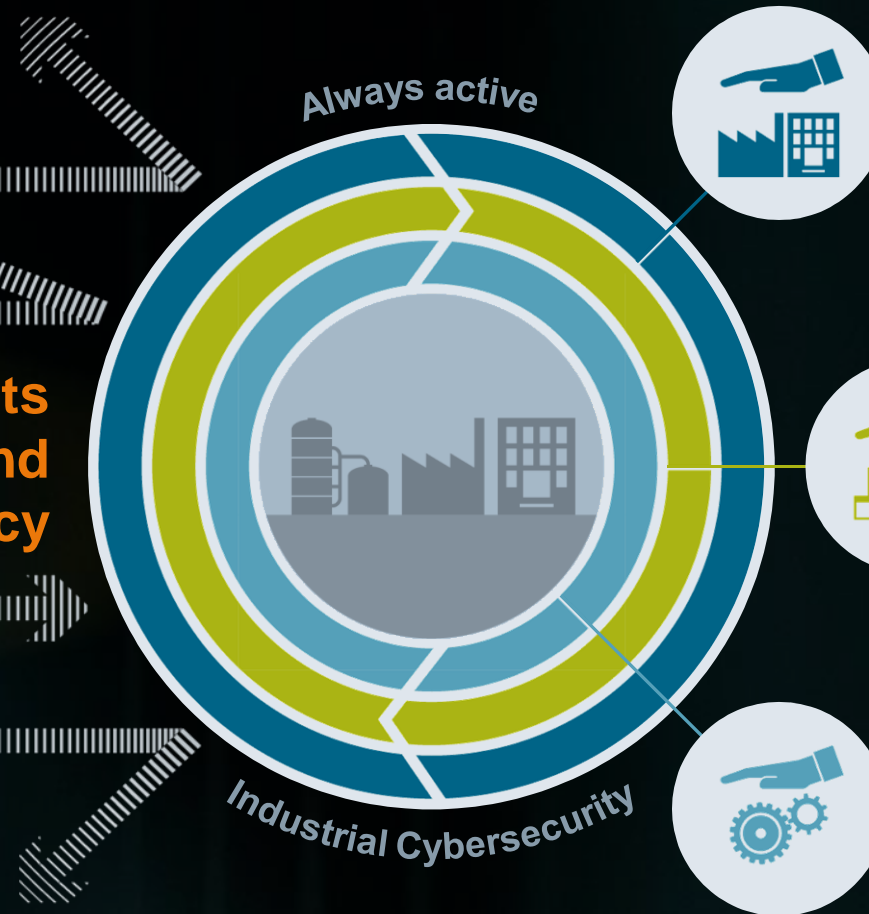


Defense-in-Depth Security Architecture based on IEC-62443

SIEMENS
Ingenuity for life

Defense in Depth

**Security threats
demand
cyber resiliency**



Plant Security

- Physical access protection
- Processes and guidelines
- Holistic security monitoring

Network Security

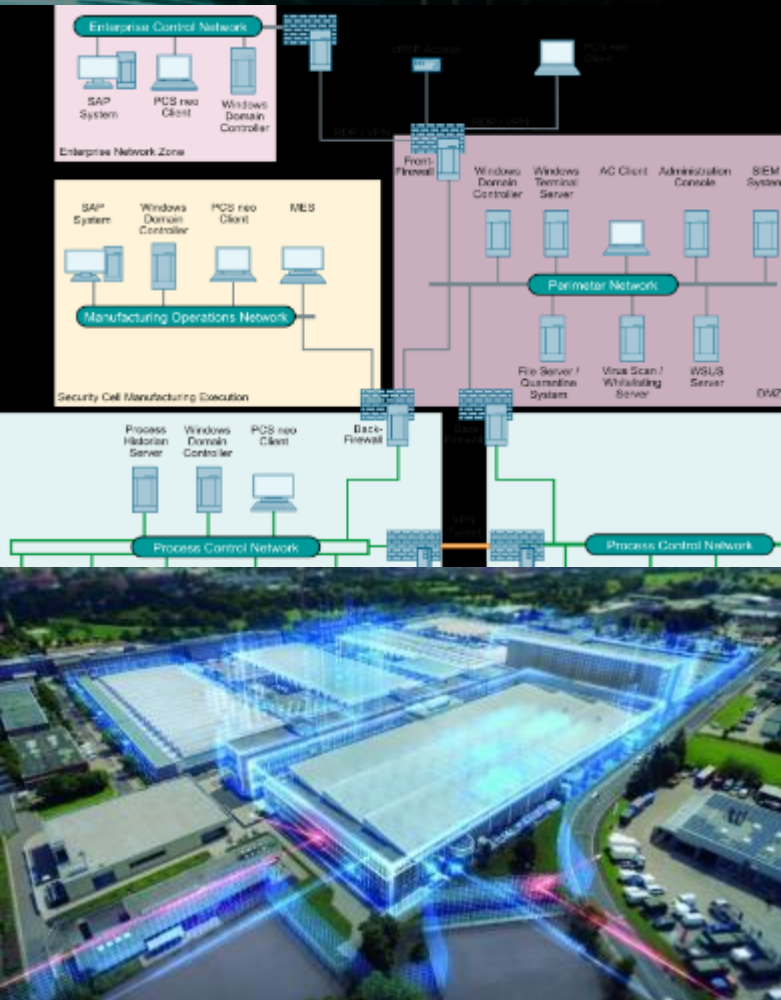
- Cell protection and perimeter network
- Firewalls and VPN

System Integrity

- System hardening
- Patch management
- Detection of attacks
- Authentication and access protection

Network Security

Network Cells, Firewalls and VPN



Logical Segregation via Network Cells

- Architect ICS assets to operate in separated network cells via physical and logical network segmentation.

Firewall Layers

- Front firewall channel to control and restrict the data exchange with the office (IT) enterprise network and the production (OT) network.
- Perimeter network (DMZ) to allow service and support access to the plant with controlled and restricted data exchange with the process control network.
- On every host Operating System (e.g. Windows) install or implement a firewall or application whitelisting to protect critical ICS application services.



Secure Remote Access (RA) should always be used when connectivity is required for teleservice and remote maintenance.

Secure

Encrypted communications via IPsec and VPN, TLS encryption, Multi-Factor Authentication.

Flexible

Protocol-independent, IP-based communication.

Accounting Management

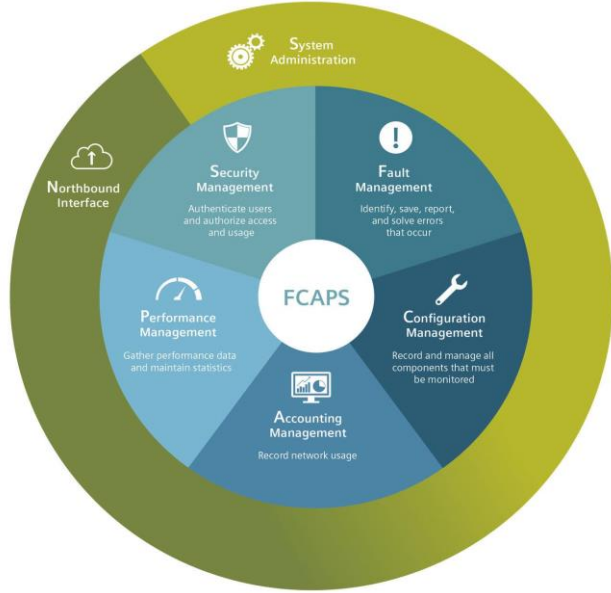
Record network usage.

Centralized Administration

Central administration of all VPN connections, simple user management, easy integration.



Siemens SINEMA Remote Connect lets you access remote ICS assets conveniently and securely, even if they're integrated to other networks.



A Network Management System (NMS) for industrial networks is critical for OT network security. The NMS supports the five pillars defined in the FCAPS model.

Fault Management

Identify, save, report, and solve any error status that occur.

Configuration Management

Record and manage all OT network components that must be monitored.

Accounting Management

Record network usage.

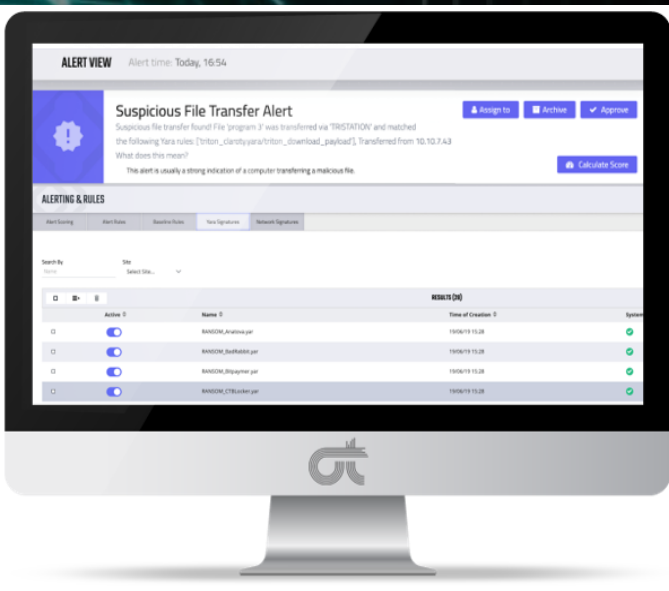
Performance Management

Gather performance data and maintain statistics.

Security Management

Authenticate users and authorize access and usage.

Siemens SINEC NMS fulfills process-based and technical security requirements according to IEC 62443 framework.



An Intrusion Detection System (IDS) for industrial networks is critical for providing continuous threat detection using

Asset Management

OT network and control system assets.

Threat and Anomaly Detection

Continuous, Near-Real-Time, Artificial Intelligence (AI) and Machine Learning.

Network Segmentation

Network zones, remote networks & sites.

Vulnerability Management

Critical Vulnerabilities & Exposures (CVEs).

IT/OT Operations

Change control, change validation, SIEM integration.

Claroty & Nozomi employ Artificial Intelligence (AI) and Machine Learning (ML) for near-real-time anomaly & continuous threat detection.

Siemens RUGGEDCOM

SIEMENS
Ingenuity for life

The Siemens RUGGEDCOM family of modular Layer 2 and Layer 3 switches, and intelligent IoT nodes offers WAN, serial or Ethernet connectivity options with embedded security.

RUGGEDCOM RX1500

Field-proven industrial network devices coupled with security applications to offer customized solutions for various security levels. Field-swappable modules for flexibility and easy maintenance for critical applications.



RUGGEDCOM APE

Industrial Application Processing Engine provides a powerful industrial application platform that lets you tap into a range of Siemens and leading 3rd party security applications in mission-critical environments.



RUGGEDCOM RX1400 IN

Industrial Intelligent Node (IoT) with advanced security features including ML user passwords, SSH/SSL (128-bit encryption), port security, firewall & IDS, VLAN (802.1Q), RADIUS, SNMPv3 and 56-bit encryption.



The Siemens SCALANCE S Industrial Security Appliances as a part of network security support the “Defense in Depth” industrial security concept. They protect automation networks, and seamlessly connect to the security structures of the Office and IT world.

Industrial Firewall Appliances

High-performance Industrial Firewall Appliances offer you versatile firewall mechanisms you can use to protect even flat networks with a throughput of 600 Mbit/s and up to 1,000 firewall rules.

Industrial VPN Appliances

In addition to the firewall mechanisms offered by the Industrial Firewall Appliances, powerful Industrial VPN Appliances also permit up to 200 VPN connections with a data throughput of up to 120 Mbit/s.



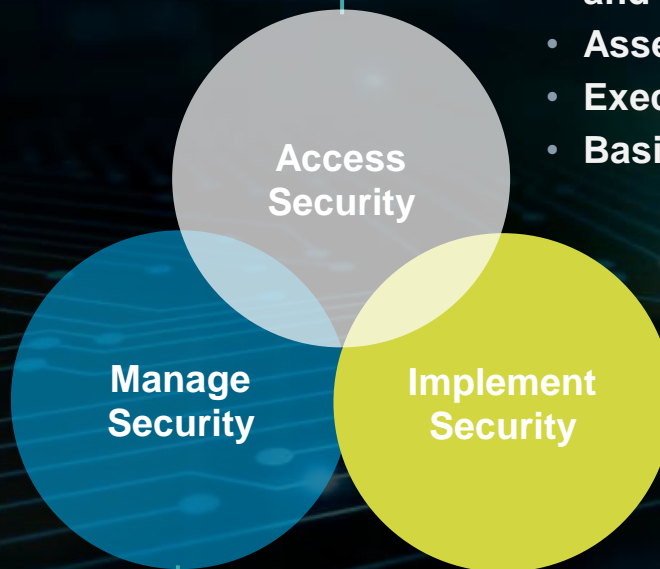
SCALANCE S is developed in accordance with the provisions of the Industrial Security Standard IEC 62443-4-1, as certified by the TÜV. These provide for the implementation of a flexible security zone concept and be used in a temperature range of -40 to +70°C.

Siemens Industrial Security Services (ISS) - Portfolio



Comprehensive security through monitoring and pro-active protection

- Close security gaps with continuous updates and backups.
- Identify and handle security incidents thanks to continuous security monitoring.
- Early adaption to changing threat scenarios.



Evaluation of current Security Status

- Analysis of threats and vulnerabilities to identify, evaluate and classify risks.
- Assessment of business and operational impacts.
- Execution from process engineering and automation view.
- Basis for the establishment of a security program.

Risk mitigation through implementation of security measures

- Design and implement technical security measures.
- Develop and deploy security relevant processes.
- Enhance security awareness with specific training.

Siemens Industrial Security Information



Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit <http://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <http://www.siemens.com/industrialsecurity>.



The image is a black and white conceptual illustration. At the bottom, a person's hands are shown typing on a laptop keyboard. Above the laptop, a large rectangular box contains the text "THANK YOU!" in a bold, sans-serif font. The background is dark and filled with various white line-art icons and data visualizations. These include: several bar charts of different sizes; line graphs showing trends; three donut charts with percentage labels (62%, 26%, 24% and 51%, 45%); a horizontal bar chart with values 12%, 8%, 14%, and 20%; a target icon with an arrow; a hexagonal grid; a cluster of three gears; a play button icon; a group of three people icon; a telephone handset icon; a pie chart; a gear icon; a series of five stars; an envelope icon; and a document icon. The entire scene is interconnected by a network of thin white lines and dots, suggesting a digital or data-driven environment.

THANK YOU!

Questions & Answers



Disclaimer



© Siemens 2020

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.