SIEMENS

Ingenuity for life

Siemens Australia ISS

Industrial Security Services

siemens.com/industrialsecurity

CLAROTY

Clarity for OT Networks

Operational Technology (OT)

Continuous Threat Detection

Bridging the IT-OT Cybersecurity Gap

Presenter Profile

SIEMENS
Ingenuity for life

Serge Maillet

Organisation	Siemens Australia
Job Function	Business Segment Manager CI & Industrial Cybersecurity
Time in Industry	21 Years
Credentials	MSc. Cybersecurity

my motto: Cybersecurity is only as strong as your weakest link.

Presenter Profile

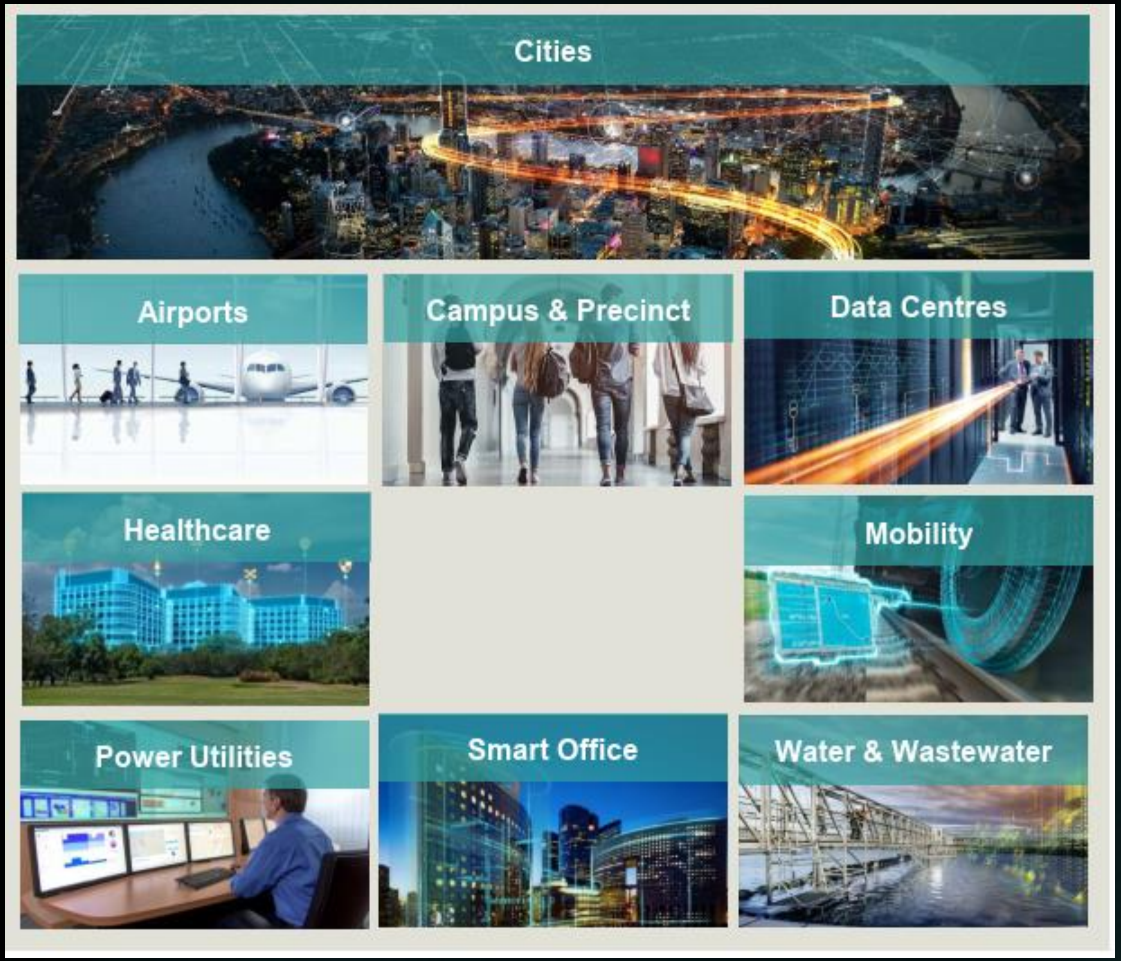
Pawel Krzysztofik

Organisation	Siemens Australia
Job Function	Principle Network Engineer
Time in Industry	22 Years
Credentials	CCIE

my motto: What happens in Brisvegas never happened.

Siemens Australia – key vertical market segments

SIEMENS
Ingenuity for life

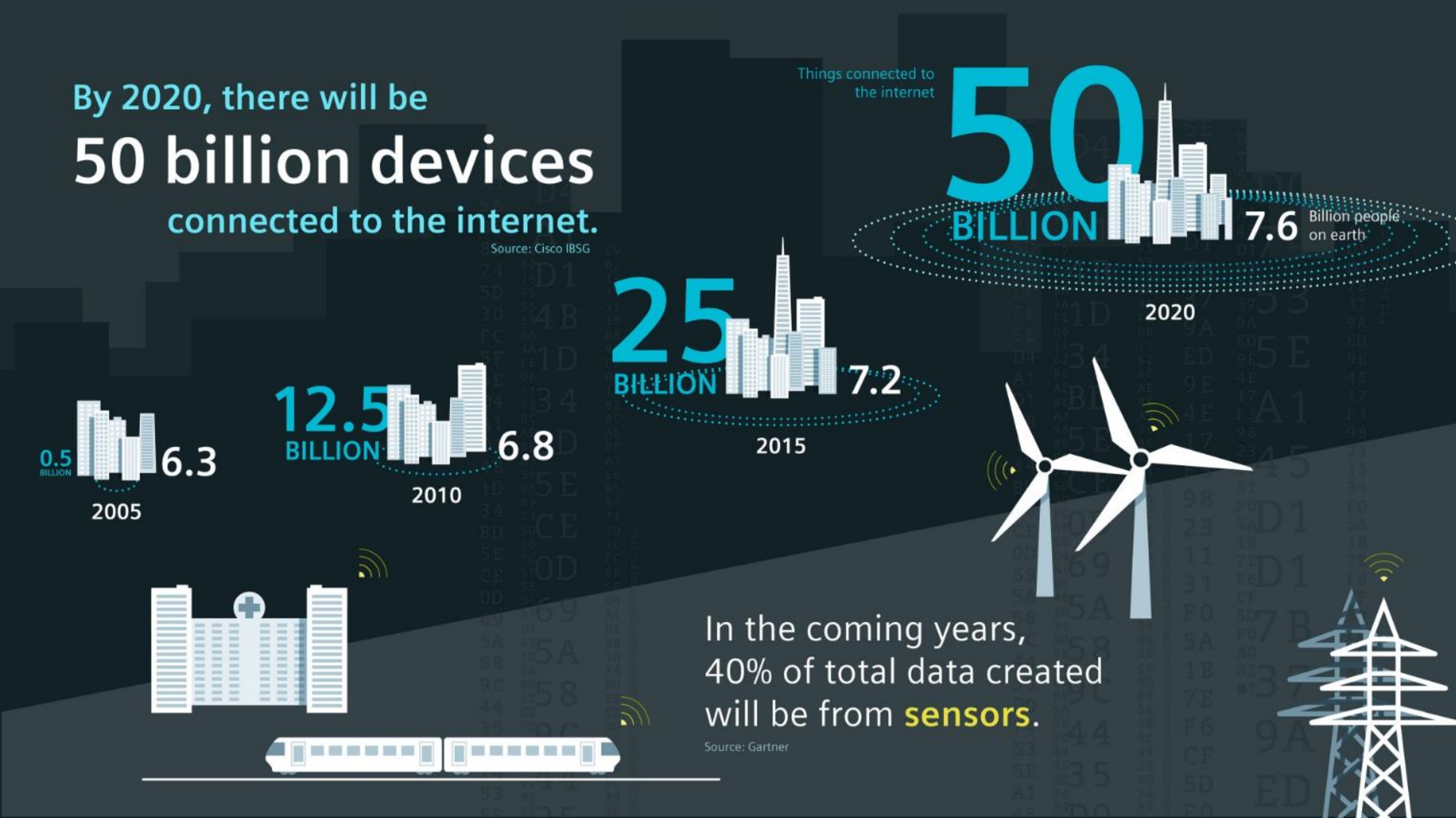


By 2020, there will be

50 billion devices

connected to the internet.

Source: Cisco IBSG



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

Source: Gartner

Cybersecurity attacks on critical infrastructure 2010 - 2018

"GreyEnergy"	2017
"Triton"–	2017
"WannaCry", "Petya" and "NotPetya"	2017
Iran petrochemical	2016
"BlackEnergy"	2015
"Energetic Bear"	2014

STUXNET
Virus
VIRUS

2010	Stuxnet
2011	Virus "Duqu"
2012	Telvent
2013	Germany steel mill ISC attack
2014	Black Energy

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

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

Cybersecurity landscape in Australia

SIEMENS
Ingenuity for life

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.

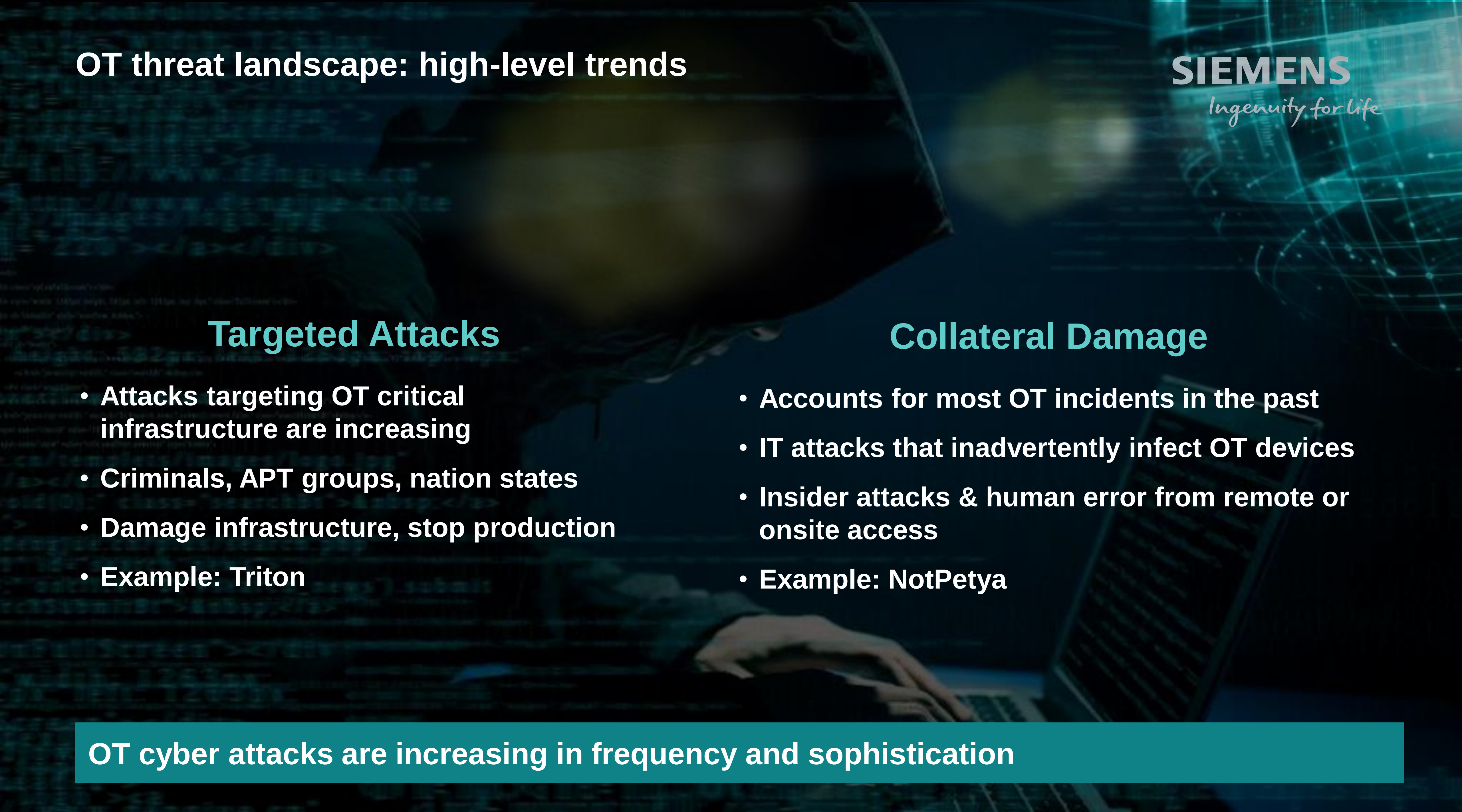
Australia currently has less than 10% of the Cybersecurity expertise that it requires to protect its industries in all industry verticals.

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.

OT threat landscape: high-level trends



Targeted Attacks

- Attacks targeting OT critical infrastructure are increasing
- Criminals, APT groups, nation states
- Damage infrastructure, stop production
- Example: Triton

Collateral Damage

- Accounts for most OT incidents in the past
- IT attacks that inadvertently infect OT devices
- Insider attacks & human error from remote or onsite access
- Example: NotPetya

OT cyber attacks are increasing in frequency and sophistication

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:

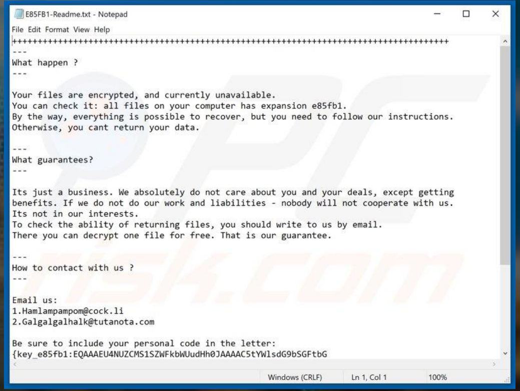
31 January, 2020 (when they became aware)

How**:**

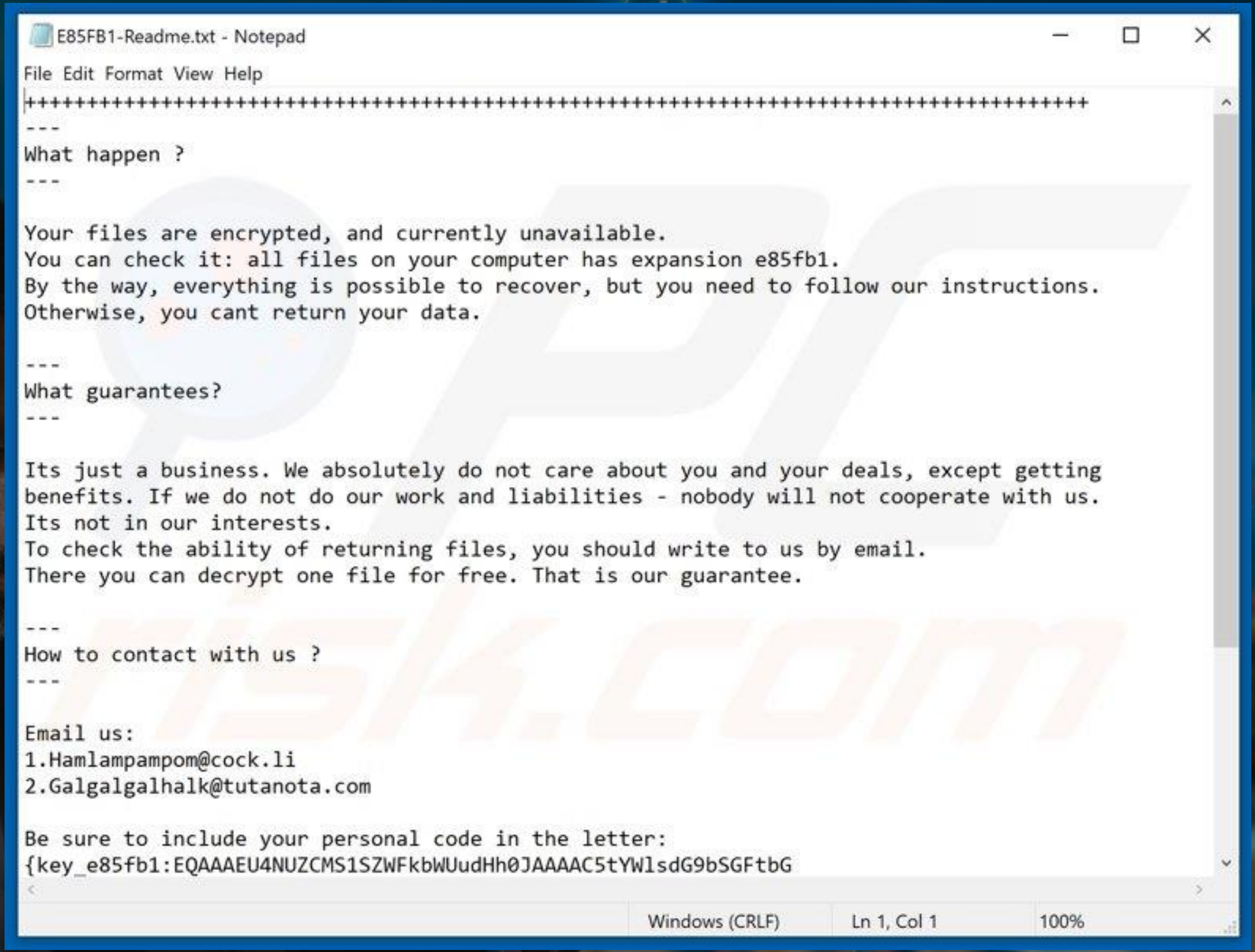
Mailto Ransomware (encrypted file systems)

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)

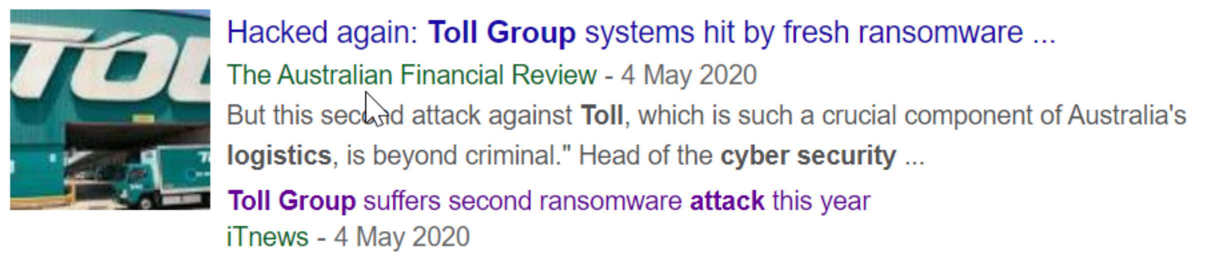


```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
---
What happen ?
---

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.Galgalgalhalk@tutanota.com

Be sure to include your personal code in the letter:
{key_e85fb1:EQAAAEU4NUZCMS1SZWFkbWUudHh0JAAAAC5tYWlsdG9bSGFtbG
```



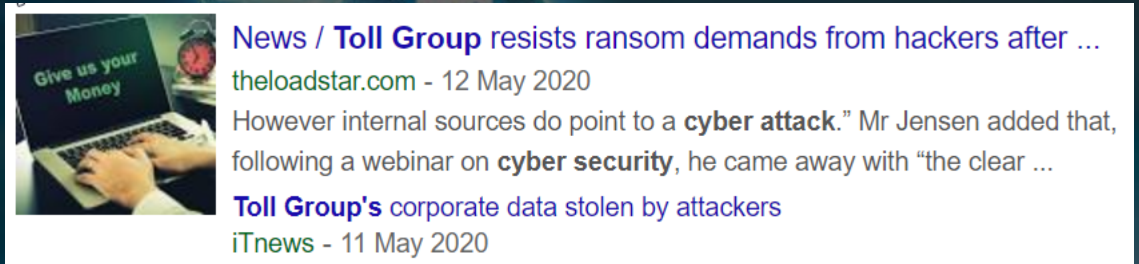
```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
---
What happen ?
---

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.Galgalgalhalk@tutanota.com

Be sure to include your personal code in the letter:
{key_e85fb1:EQAAAEU4NUZCMS1SZWFkbWUudHh0JAAAAC5tYWlsdG9bSGFtbG
```

Update: Toll Group attacked again with ransomware in May 2020.



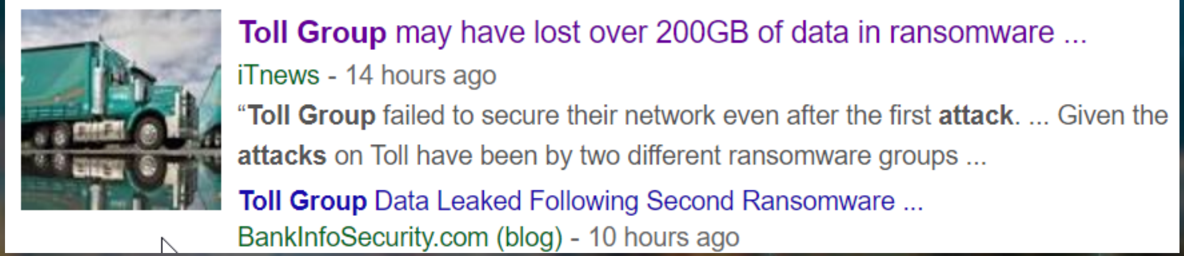
Hacked again: **Toll Group** systems hit by fresh ransomware ...
The Australian Financial Review - 4 May 2020
But this second attack against **Toll**, which is such a crucial component of Australia's **logistics**, is beyond criminal." Head of the **cyber security** ...

Toll Group suffers second ransomware **attack** this year
iTnews - 4 May 2020



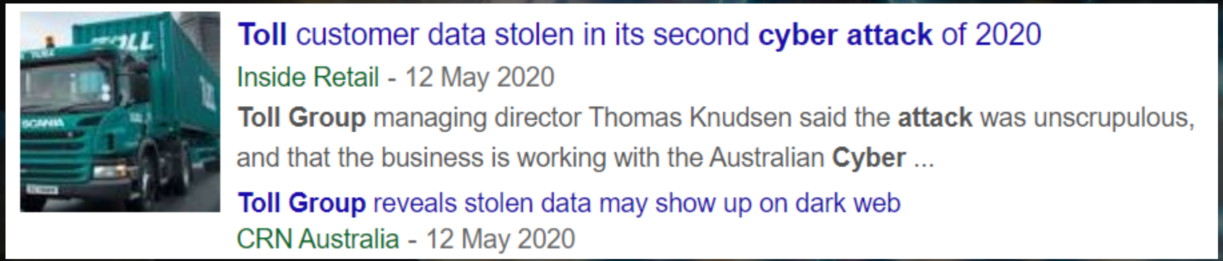
News / **Toll Group** resists ransom demands from hackers after ...
theloadstar.com - 12 May 2020
However internal sources do point to a **cyber attack**." Mr Jensen added that, following a webinar on **cyber security**, he came away with "the clear ...

Toll Group's corporate data stolen by attackers
iTnews - 11 May 2020



Toll Group may have lost over 200GB of data in ransomware ...
iTnews - 14 hours ago
"**Toll Group** failed to secure their network even after the first **attack**. ... Given the **attacks** on Toll have been by two different ransomware groups ...

Toll Group Data Leaked Following Second Ransomware ...
BankInfoSecurity.com (blog) - 10 hours ago



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

Top 5 Vulnerabilities, Risks and Exposures for Digital Industry

SIEMENS
Ingenuity for life

1. Industrial Control Systems (ICS) software applications and operating systems are outdated and vulnerable to CVEs.
2. Industrial networks are ineffectively segregated.
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.

OT Security is a requirement for organisations

OT is uniquely susceptible to cyber attacks

- Historically insecure by design
- IT/OT convergence exacerbates insecurities
- Vulnerable to “spillover” attacks from IT
- Desirable targets for threat actors

High potential for significant negative impact

- Downtime & operational disruption
- Financial & reputational damage
- Compliance violations
- Safety risk

Enterprises require comprehensive security for their OT environments

Gartner

Operational technology is increasingly connected to corporate IT networks, meaning threats traditionally only appearing in IT now can permeate OT as well. Security and risk management leaders should implement foundational controls to stop these threats from jeopardizing their OT.

Gartner, 27 July 2018, Document: G00348833

OT Security is particularly challenging

SIEMENS
Ingenuity for life

- No Risk Baseline
- Unfamiliar Assets & Proprietary Protocols
- Insecure by Design
- IT Security Solutions Directly Incompatible with OT
- Dependency on OT staff
- Limited Connectivity
- Onerous Change Control Procedures

Digital Transformation drives OT security with CISO

SIEMENS
Ingenuity for life

64% of leaders note that slowing digital transformation for any reason can compromise their competitive edge

62% of leaders are increasing their cybersecurity budgets to address OT security risk

70% of organisations will roll OT security under the CISO in 2020

However, 78% of organisations still have limited OT visibility

> “Organisations should seek security solutions that work together to provide broad visibility of the entire digital attack surface, spanning OT and IT environments.”

CLAROTY
Clarity for OT Networks

Key components of an effective OT security strategy

SIEMENS
Ingenuity for life

Credible

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

Deep OT awareness for accurate risk assessment.

Efficient

Integrate into existing processes and workflows

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

Non-Disruptive

Avoid distracting IT staff with complex tools and technology

Create absolute minimum risk to production availability.

Gartner

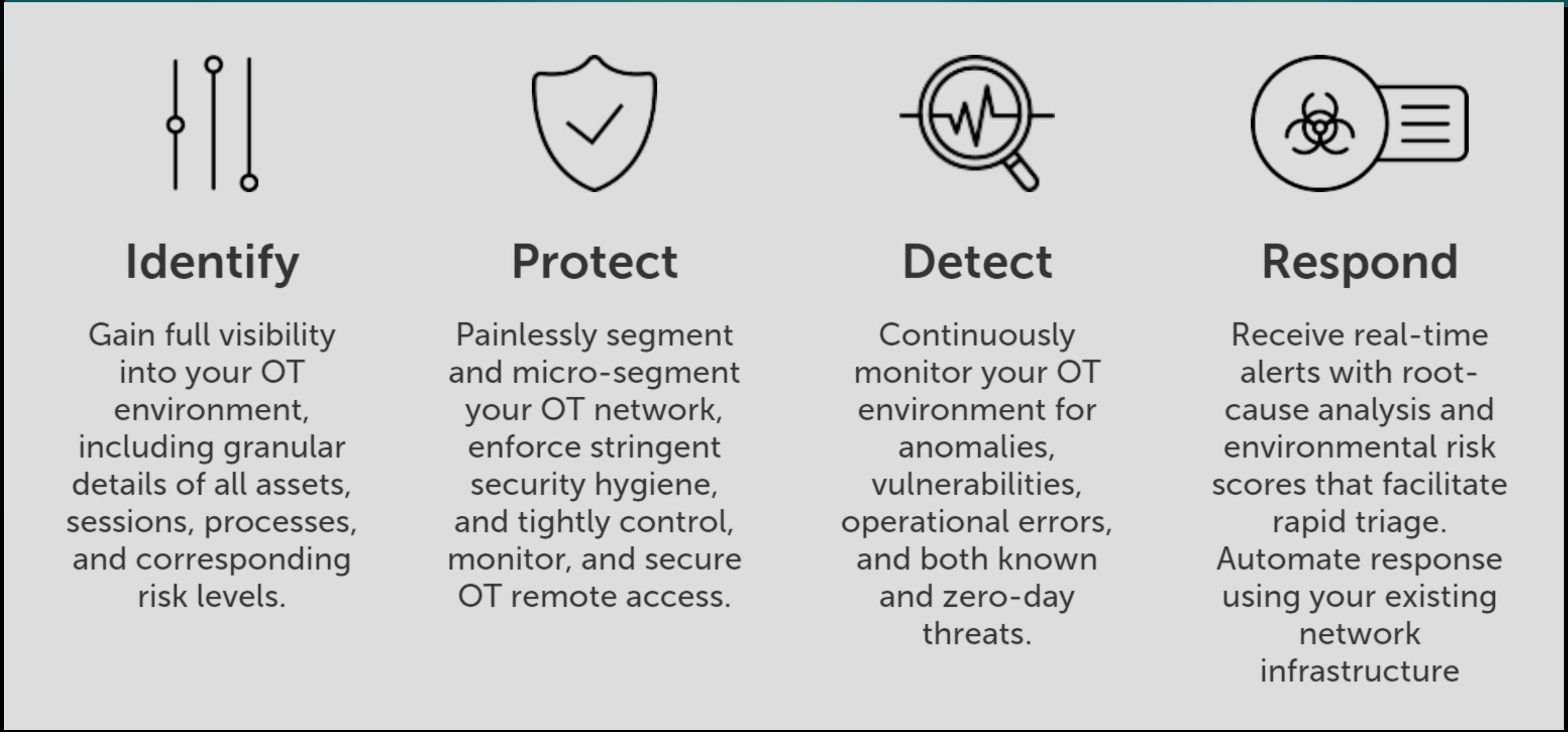
"Implementing effective security governance in an integrated IT/OT environment is difficult because the two domains have different risk appetites and security requirements. Security and risk management leaders need a single governance structure to support both domains and balance their requirements."

Gartner, 10 October 2019, Document: G00441788

CLAROTY
Clarity for OT Networks

Introducing the Claroty platform

Comprehensive OT Security & Actionable Intelligence



Identify

Gain full visibility into your OT environment, including granular details of all assets, sessions, processes, and corresponding risk levels.

Protect

Painlessly segment and micro-segment your OT network, enforce stringent security hygiene, and tightly control, monitor, and secure OT remote access.

Detect

Continuously monitor your OT environment for anomalies, vulnerabilities, operational errors, and both known and zero-day threats.

Respond

Receive real-time alerts with root-cause analysis and environmental risk scores that facilitate rapid triage. Automate response using your existing network infrastructure

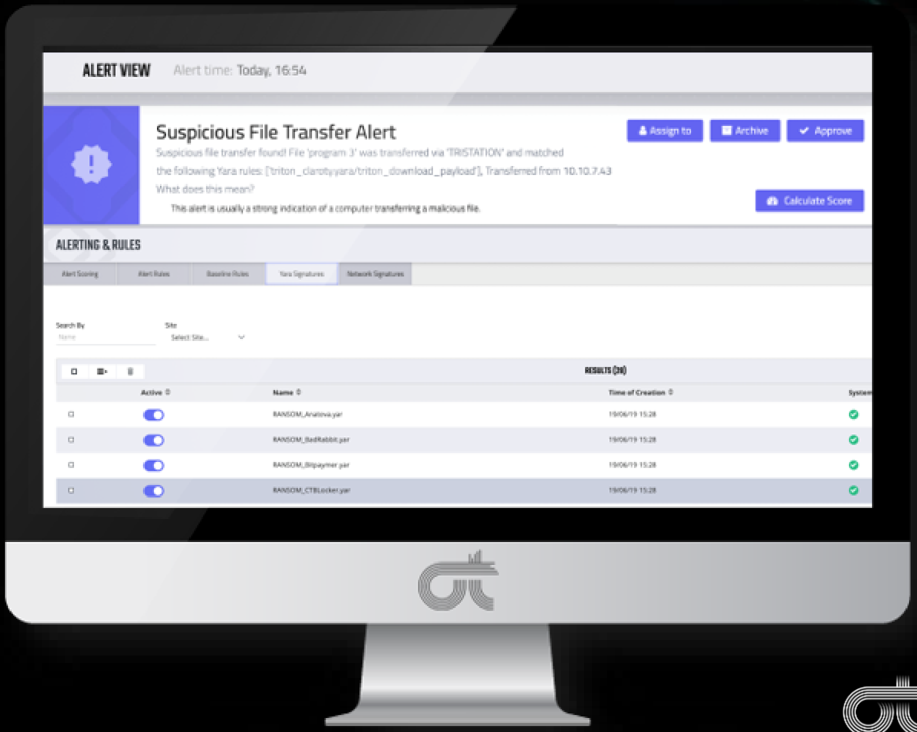
The Claroty Platform

SIEMENS
Ingenuity for life

Claroty platform capabilities

- *OT Visibility & Asset Management*
- *Threat & Anomaly Detection*
- *Network Segmentation*
- *Vulnerability Management*
- *Secure Remote Access*

Integrated End-to-End Security



ALERT VIEW Alert time: Today, 16:54

Suspicious File Transfer Alert

Suspicious file transfer found! File 'program 3' was transferred via 'TRISTATION' and matched the following Yara rules: ['triton_claroty.yara/triton_download_payload'], Transferred from 10.10.7.43

What does this mean?

This alert is usually a strong indication of a computer transferring a malicious file.

ALERTING & RULES

Search By: Name

Site: Select Site...

RESULTS (28)

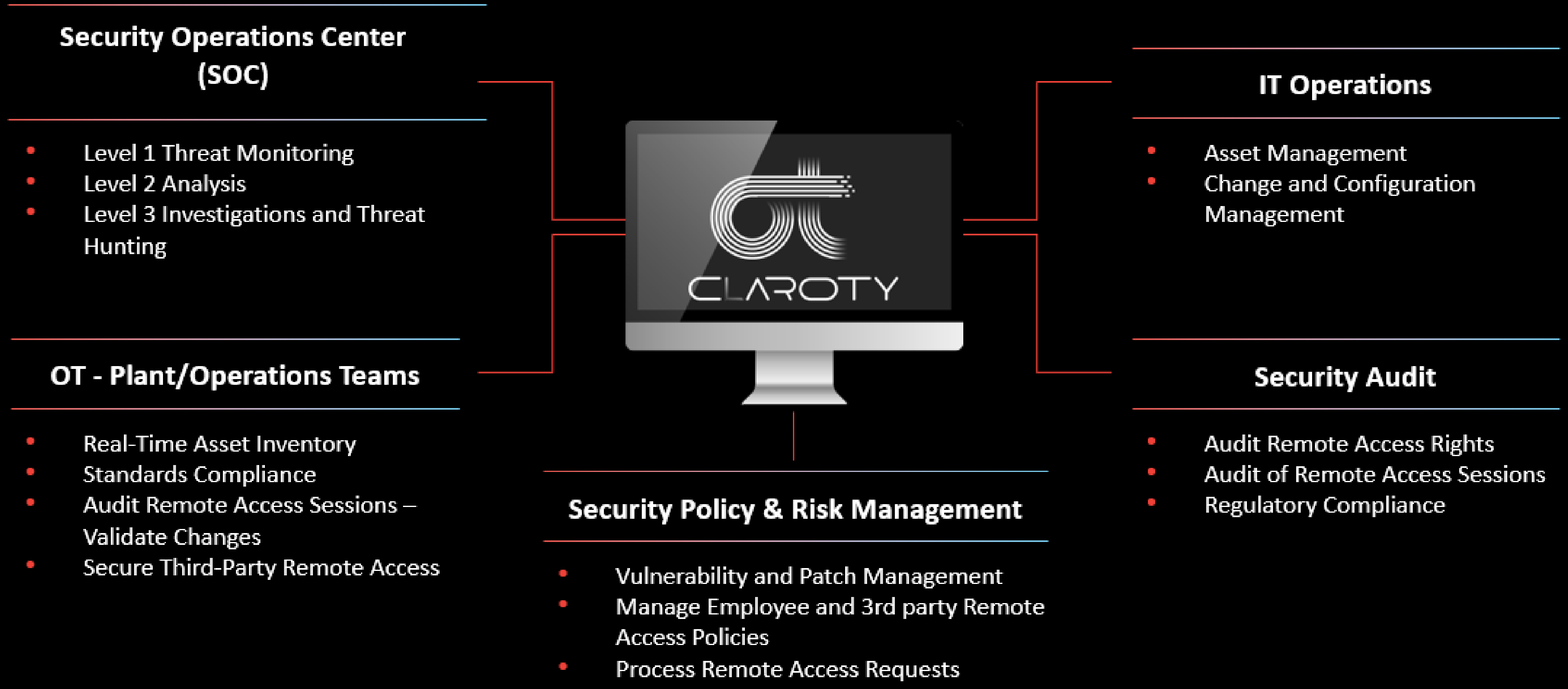
	Active	Name	Time of Creation	System
□	●	RANSOM_Anatova.yar	19/06/19 15:28	✓
□	●	RANSOM_BadRabbit.yar	19/06/19 15:28	✓
□	●	RANSOM_Bitpaymer.yar	19/06/19 15:28	✓
□	●	RANSOM_CTBLocker.yar	19/06/19 15:28	✓

CLAROTY
Clarity for OT Networks

The Claroty Platform

SIEMENS
Ingenuity for life

Support for Multiple Teams & Use Cases



Security Operations Center (SOC)

- Level 1 Threat Monitoring
- Level 2 Analysis
- Level 3 Investigations and Threat Hunting

OT - Plant/Operations Teams

- Real-Time Asset Inventory
- Standards Compliance
- Audit Remote Access Sessions – Validate Changes
- Secure Third-Party Remote Access

IT Operations

- Asset Management
- Change and Configuration Management

Security Audit

- Audit Remote Access Rights
- Audit of Remote Access Sessions
- Regulatory Compliance

Security Policy & Risk Management

- Vulnerability and Patch Management
- Manage Employee and 3rd party Remote Access Policies
- Process Remote Access Requests

CLAROTY
Clarity for OT Networks

Claroty customers and industry verticals

SIEMENS
Ingenuity for life

Sample Customers:

ABInBev
380 Sites, 7 Regions,
SOC Enablement

China Light & Power
65 Sites, 3 Regions,
SOC Enablement

The Coca Cola Company
>100 Sites,
Multiple Bottlers

Pfizer
65 Sites,
Global Rollout

BHP
50+ Sites, 3 Regions,
SOC enablement

Schneider Electric
200 Sites, 3 Regions,
SOC Enablement

- 3/10 top **Consumer Goods** Companies
- 3/10 top **Pharmaceutical** Companies
- 4/10 top **Electric Utilities** Companies
- 5/10 top **Food & Beverage** Companies
- 5/10 top **Oil & Gas** Companies
- 10/20 top **Manufacturing** Companies

Customer Verticals: 18+

Manufacturing	Offshore	Electric	Oil & Gas	Food & Bev	Real Estate
Data Centers BMS	Retail	Wind	Automotive	Pharma	Govt
Agriculture	Mining	Water	Chemical	Aerospace	Transportation

Customer Countries: 50+

CLAROTY
Clarity for OT Networks

Claroty OT security research

Best-In-Class OT Security Research Team

Claroty has the industry's leading and award-winning OT security research department. The department is divided into two teams with specific domain expertise that conduct research in coordination with the world's largest industrial automation and control providers

Industrial Control System (ICS) Protocol and Vulnerability Research to Help Detect and Remediate Flaws in Some of the World's Most Critical Infrastructure

Data and Threat Research to Extract Correlative Data out of Analyzed Systems to Provide Insights and Produce Dedicated Threat Reports

Pwn2Own MIAMI

Only Vendor Achieved 4 Exploits

ICS

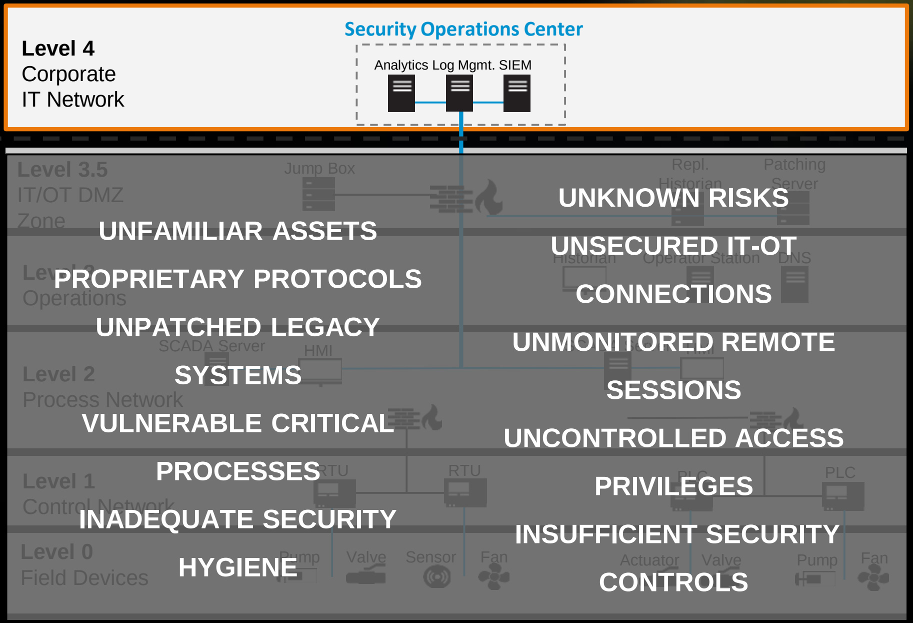
DEF CON 27 CTF Winners

S4x19

CTF Winners

Claroty provides full visibility to your previously invisible OT infrastructure

Typical OT Network → OT Network with Claroty Platform



UNFAMILIAR ASSETS

PROPRIETARY PROTOCOLS

UNPATCHED LEGACY SYSTEMS

VULNERABLE CRITICAL PROCESSES

INADEQUATE SECURITY HYGIENE

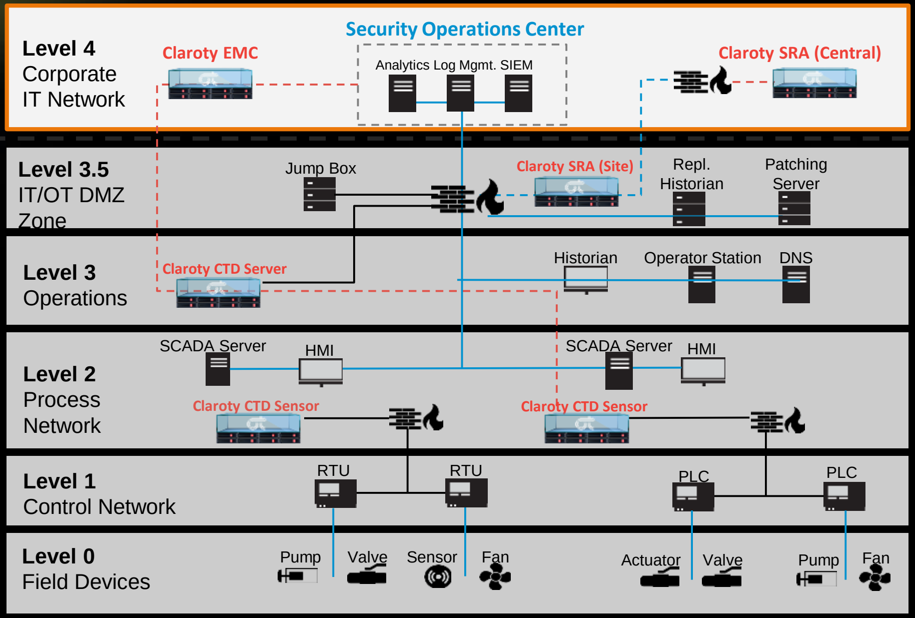
UNKNOWN RISKS

UNSECURED IT-OT CONNECTIONS

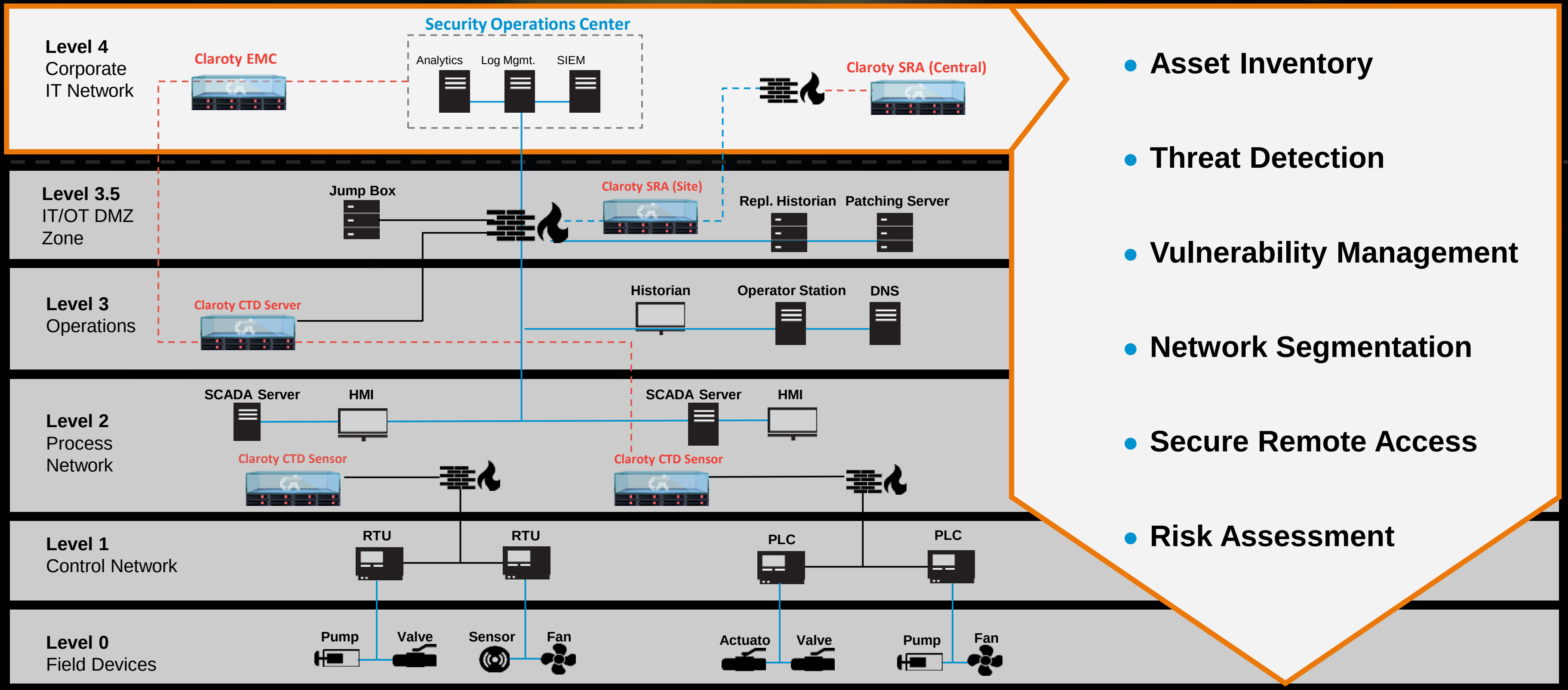
UNMONITORED REMOTE SESSIONS

UNCONTROLLED ACCESS PRIVILEGES

INSUFFICIENT SECURITY CONTROLS

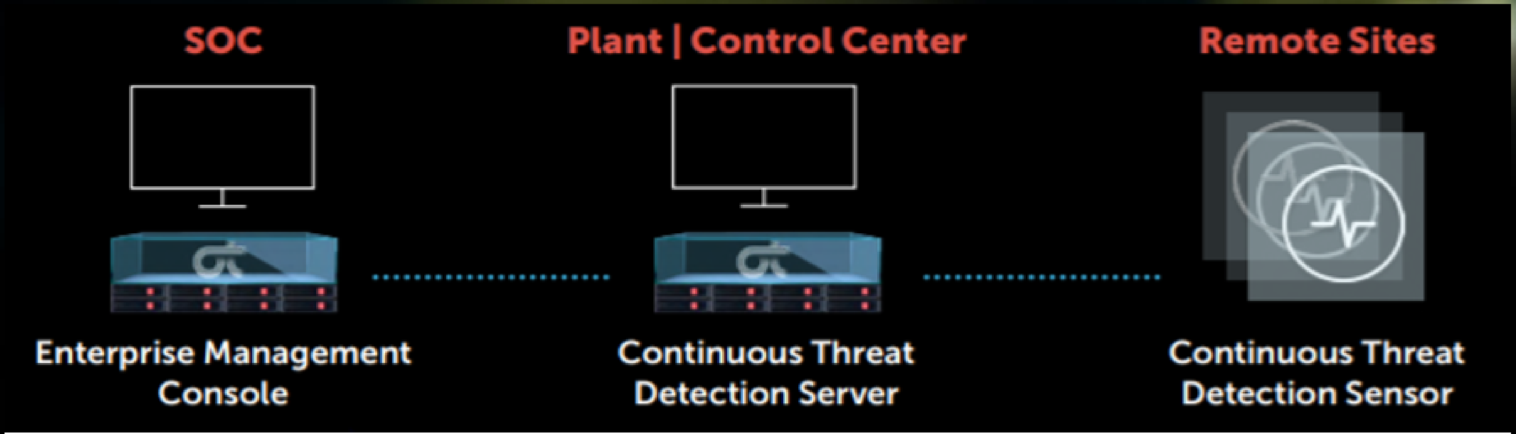


Claroty extends existing IT controls to the OT environment



- Asset Inventory
- Threat Detection
- Vulnerability Management
- Network Segmentation
- Secure Remote Access
- Risk Assessment

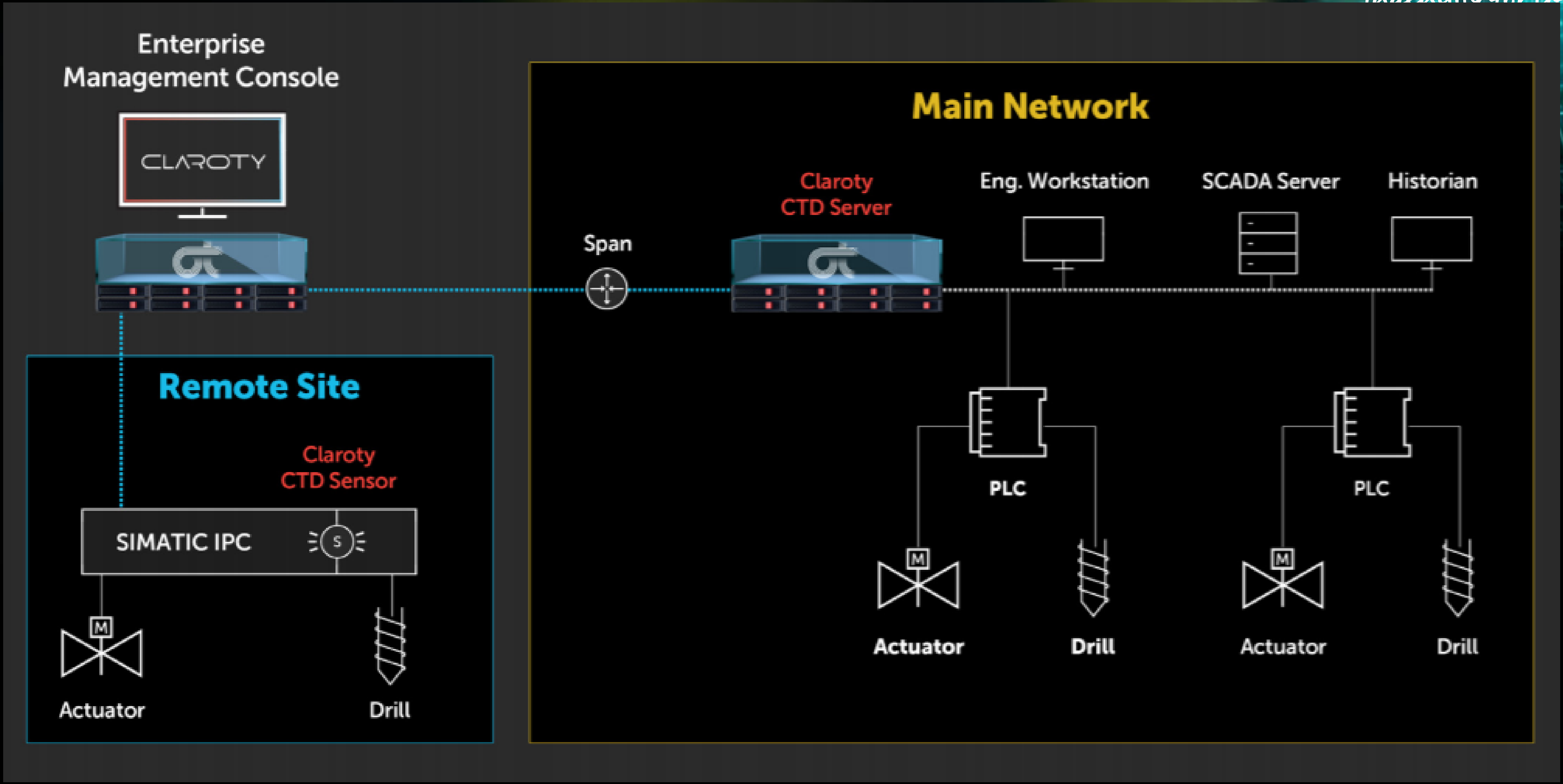
Claroty platform components


SOC
Plant | Control Center
Remote Sites
Enterprise Management Console
Continuous Threat Detection Server
Continuous Threat Detection Sensor

Enterprise Management Console (EMC)	Continuous Threat Detection (CTD) Server	Continuous Threat Detection (CTD) Sensor
Provides the centralised management interface that consolidates data from Claroty products across multiple sites, and displays a unified view of assets, activities and alerts, making it highly suitable for SOC deployments.	Provides deep visibility and extreme detection capabilities across complex multi-vendor OT environments. The server offers customers the ability to ingest sensor data and perform control functions within the distributed network infrastructure	Provides a secure and easy deployment + powerful services for rapid, reliable, and bandwidth optimised communication with the CTD server. By leveraging distributed computing power, it allows reducing the load on the CTD server.

Claroty – Siemens Reference Architecture

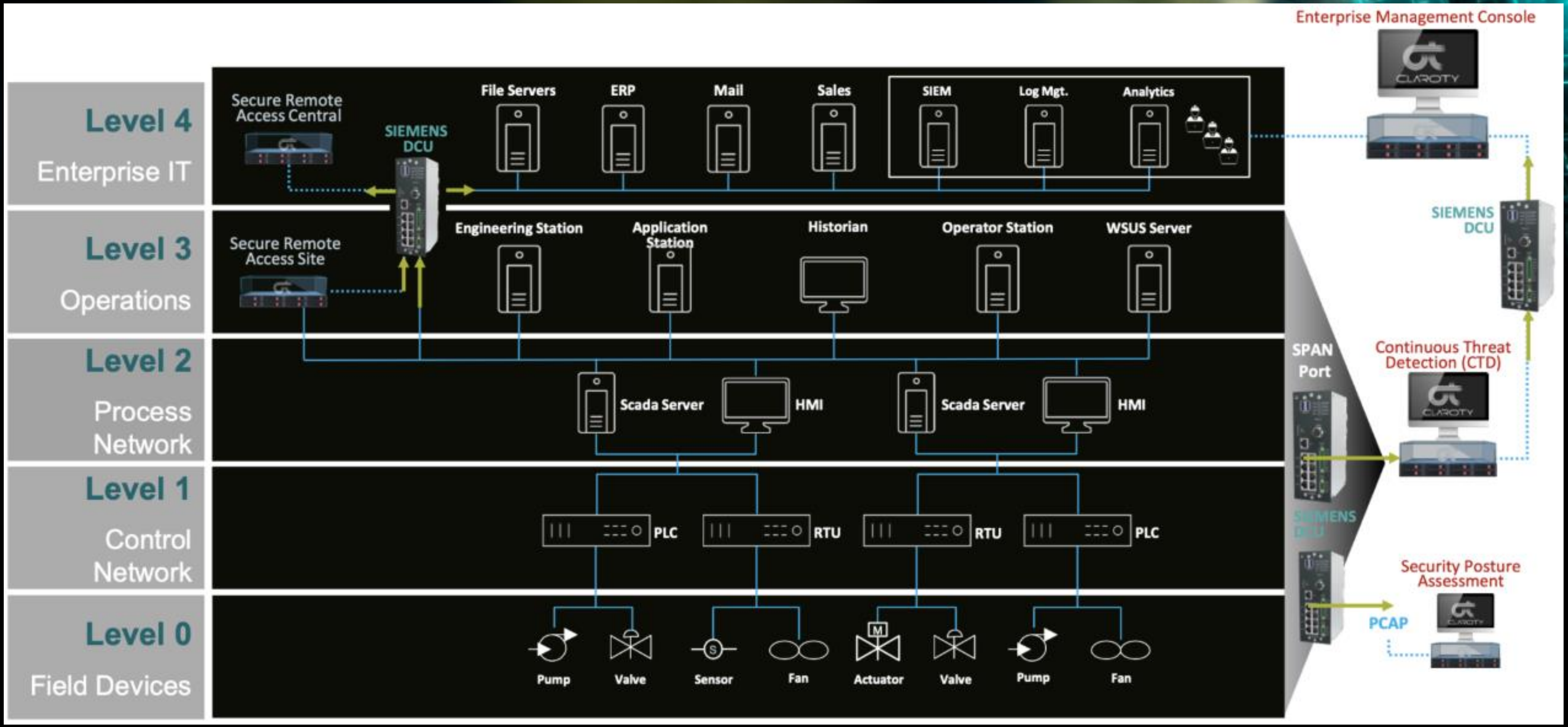
SIEMENS
Ingenuity for life



Unrestricted © Siemens 2020

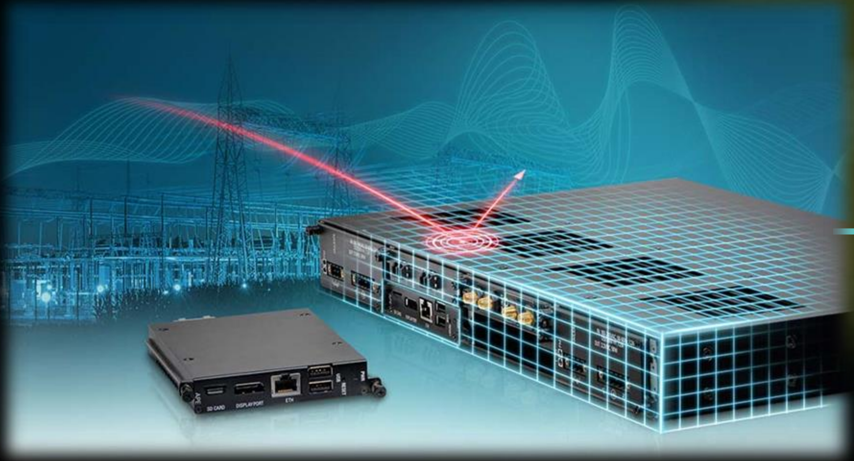
CLAROTY
Clarity for OT Networks

Claroty – Siemens Reference Architecture

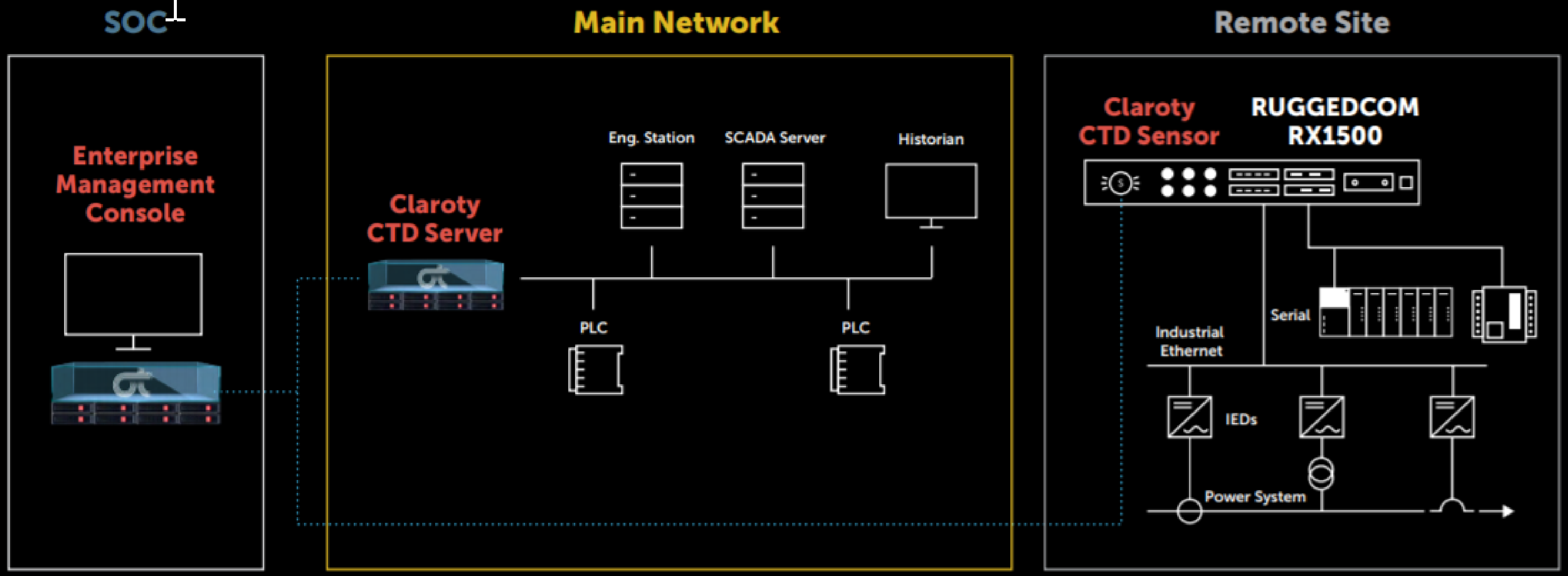


Claroty integration on Siemens RUGGEDCOM RX1500 APE

SIEMENS
Ingenuity for life



RUGGEDCOM
A Siemens Business



Unrestricted © Siemens 2020

CLAROTY
Clarity for OT Networks

Claroty Case Study 1: Manufacturing

Customer	• Global automotive manufacturer that produces thousands of cars daily across multiple global locations
Needs	• Full OT visibility integrated with existing asset discovery and management databases • Proactive detection and mitigation of potential threats in real-time • IT-OT collaboration and alignment with the SOC and existing security infrastructure
Challenges	• Limited knowledge of OT security • Historically managed and tracked asset inventory manually via error-prone spreadsheets • Thousands of geographically-dispersed assets utilizing numerous different communication protocols • Fast-paced production environment with no tolerance of downtime
Solution	• The Claroty Platform was deployed on top of existing OT infrastructure and integrated seamlessly with existing IT security infrastructure
Outcome	• CTD immediately discovered and classified all OT assets, providing a live window into the company's environment without the need for manual inventory tracking • Integrating the platform with existing OT and IT security infrastructure enabled the company to create a highly effective and unified IT-OT SOC, greatly improving alignment and collaboration across IT and OT security • Comprehensive OT visibility, as well as real-time threat detection and vulnerability monitoring, enabled the company to proactively protect against security incidents that could impact the availability, reliability, and safety of its production environment

Claroty Case Study 2: Electrical Utilities

Customer	• Leading power generation company in the electric utilities industry with multiple power plants spread across multiple regions
Needs	• Automatically identify and manage all OT assets across these plants • Continually monitor for relevant threats and exact-match vulnerabilities • Secure OT networks and assets across all power plants and minimize the risk of facing a successful attack
Challenges	• As critical infrastructure, power generation plants remain a highly desirable target for threat actors • Rising interconnectivity between OT-controlled automation systems and the IT network has created an ever-expanding attack surface • Limited insight into existing vulnerabilities & vectors an attacker could exploit in order to compromise operations • Limited visibility into OT networks and assets due to prevalence of propriety protocols, geographically dispersed plants, and lack of suitable monitoring and detection tools
Solution	• The Claroty Platform was deployed on top of existing OT network infrastructure at each plant and then integrated with the SIEM & SOAR platforms used by the company's SOC
Outcome	• CTD rapidly discovered, classified, and established a behavioral baseline for all OT assets across the company's power plants • The platform's attack vector mapping feature enabled the SOC to quickly identify and mitigate two highly vulnerable attack vectors • Armed with these capabilities, the SOC was able to proactively identify and protect critical assets, thereby significantly reducing the risk of a plant facing a successful attack in the future

CLAROTY
Clarity for OT Networks

SIEMENS

CLAROTY

Clarity for OT Networks

SIEMENS
Ingenuity for life

Disclaimer

SIEMENS
Ingenuity for life

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.