Uvod u sajber bezbednost SCADA sistema

Ivan Mladenović, Regional Manager Adriatic

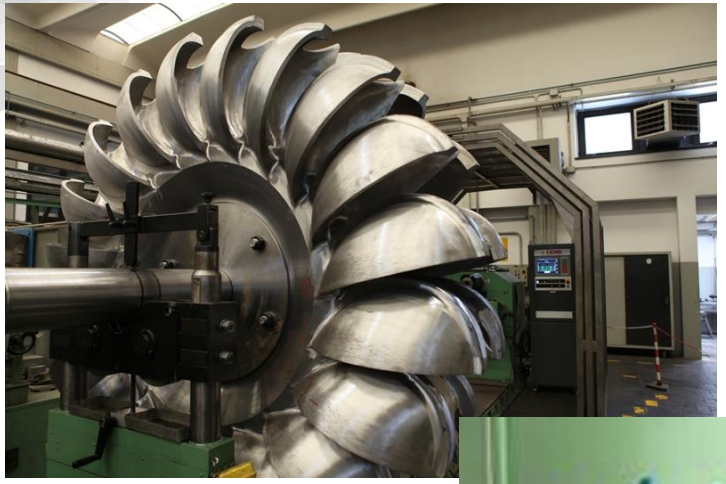
Nikola Markovinović, Security Engineer

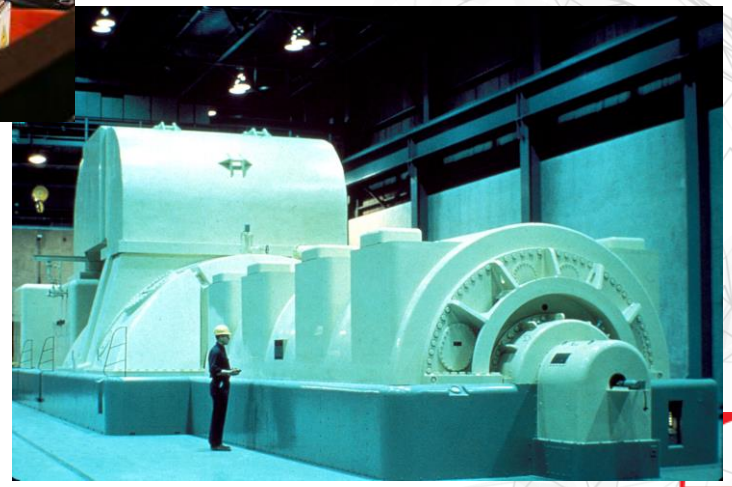
Agenda

1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

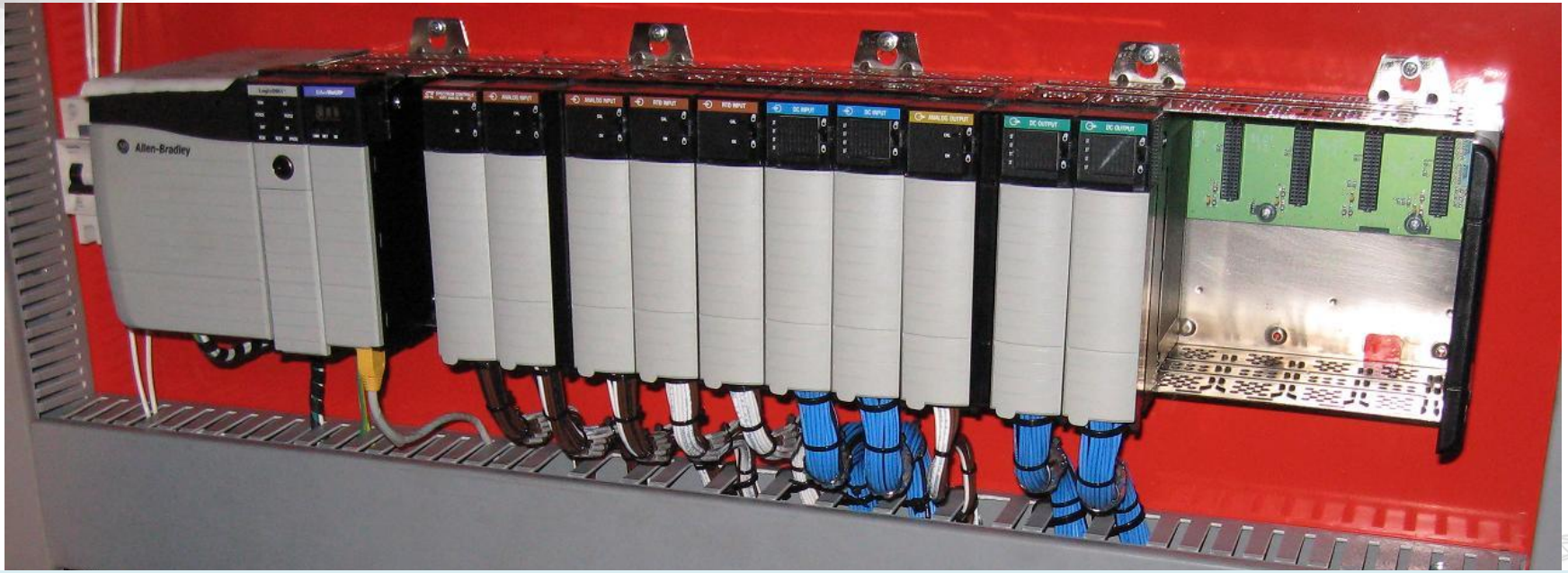
1. **SCADA, ICS, OT – terminology and meaning**
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

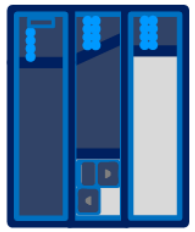
Industrial machinery and equipment





CLICO





Control devices

- PLC - Programmable Logic Controller
- PAC - Programmable Automation Controller
- RTU - Remote Terminal Unit

Industrial machinery and equipment

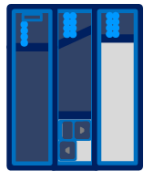
ICS - Industrial Control System = IACS - Industrial Automation and Control System

Advanced analytics and data storage

- MES – Manufacturing Execution System
- APC - Advanced Process Control
- Data Historian

Visualization, supervision and control

- SCADA - Supervisory Control and Data Acquisition
- DCS - Distributive Control System
- HMI - Human Machine Interface



Control devices

- PLC - Programmable Logic Controller
- PAC - Programmable Automation Controller
- RTU - Remote Terminal Unit

OT - Operational Technology

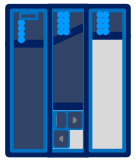
ICS - Industrial Control System = IACS - Industrial Automation and Control System

Advanced analytics and data storage

- MES – Manufacturing Execution System
- APC - Advanced Process Control
- Data Historian

Visualization, supervision and control

- SCADA - Supervisory Control and Data Acquisition
- DCS - Distributive Control System
- HMI - Human Machine Interface



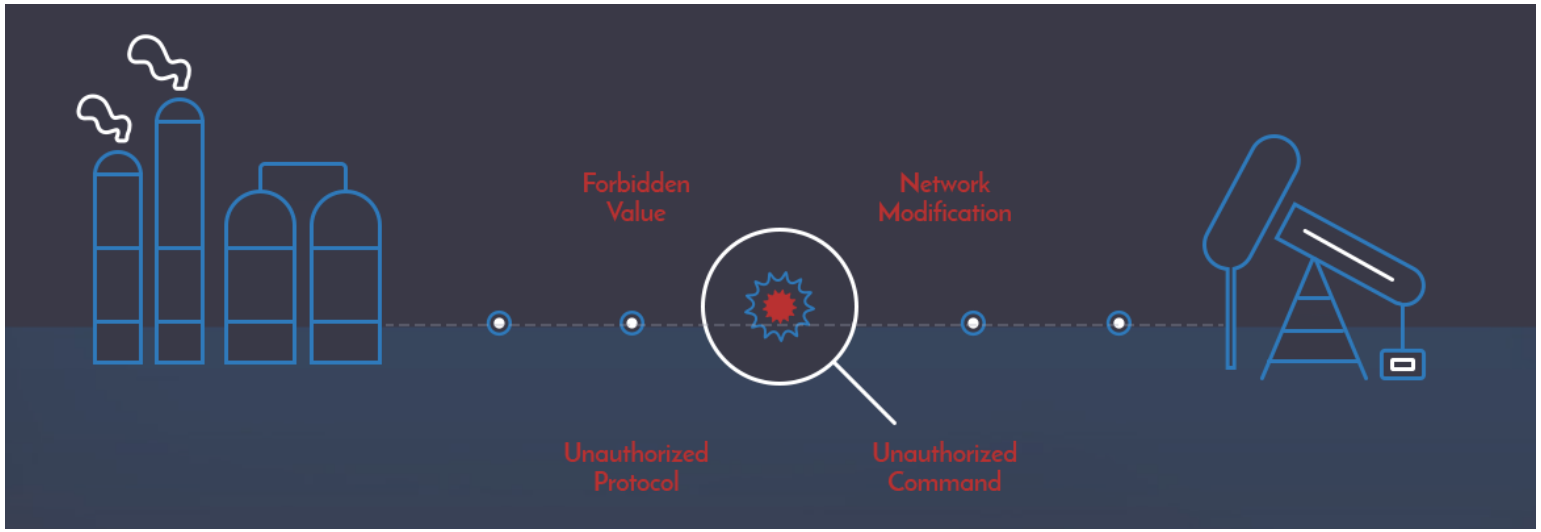
Control devices

- PLC - Programmable Logic Controller
- PAC - Programmable Automation Controller
- RTU - Remote Terminal Unit

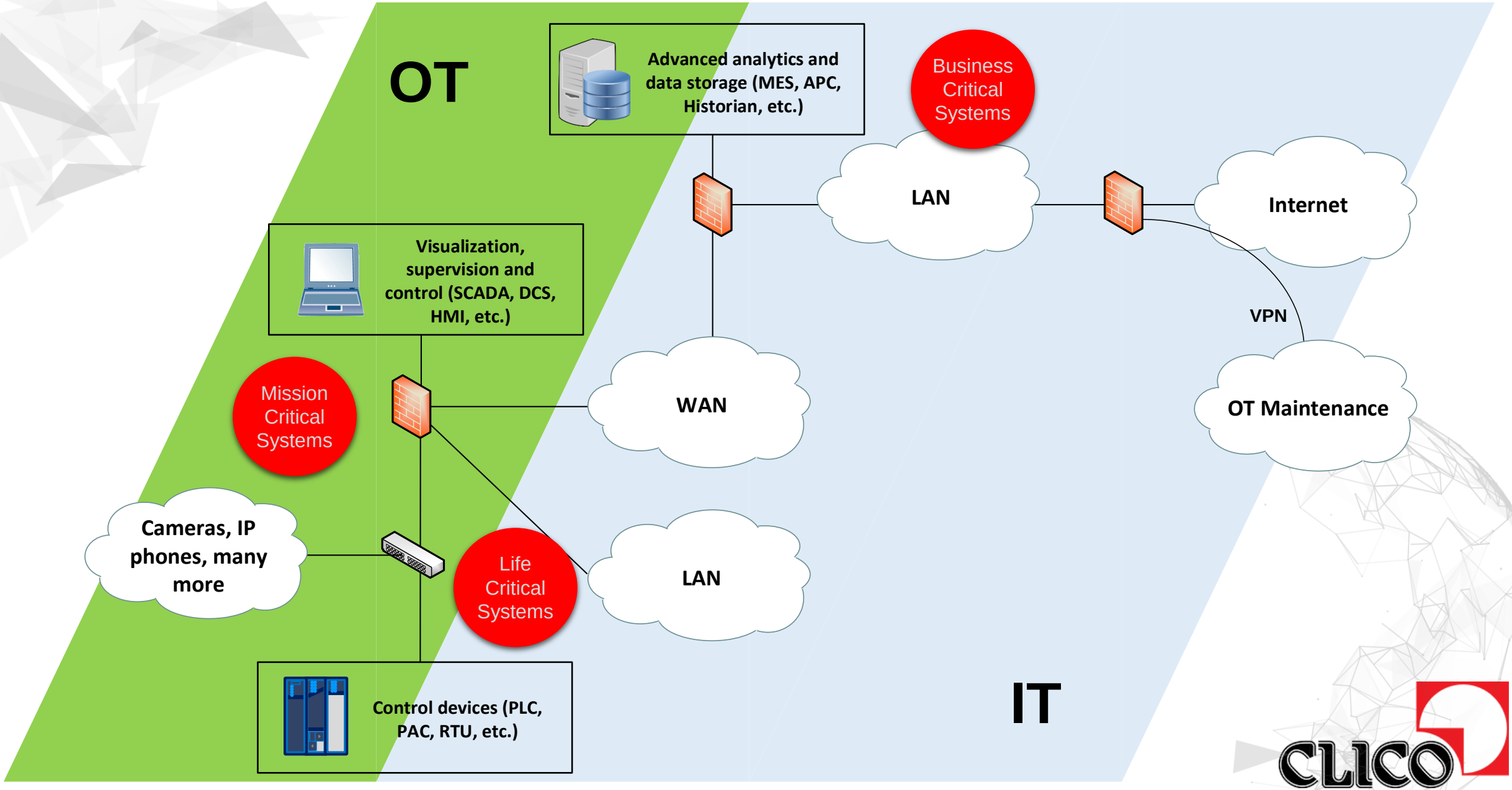
Industrial machinery and equipment

What is SCADA security?

SCADA security is the practice of protecting supervisory control and data acquisition (SCADA) networks, a common framework of control systems used in industrial operations. These networks are responsible for providing automated control and remote human management of essential commodities and services such as water, natural gas, electricity and transportation to millions of people. They can also be used to improve the efficiencies and quality in other less essential (but some would say very important!) real-world processes such as snowmaking for ski resorts and beer brewing. SCADA is one of the most common types of industrial control systems (ICS).



Business-critical	Systems that failure can cause significant tangible or intangible economic costs, e.g., customer accounting system in a bank, ERP system, etc.
Security-critical	Systems that deal with large datasets of sensitive data, e.g., PII covered by GDPR.
Mission-critical	Systems that failure can cause an inability to complete the overall system or project objectives; e.g., loss of navigation of a spacecraft, unavailability of an important industrial process, etc.
Life-critical, safety-critical	Systems that failure can cause loss of life, serious personal injury, or damage to the natural environment.
Critical infrastructure	Assets that are essential for the functioning of a society and economy, e.g., electricity generation, transmission and distribution, water supply, public health, transportation systems, telecommunication, banking and financial services, etc.



Network and Information Security Directive (NISD)

Organizations impacted	• **Operators of essential services** in the energy, transport, banking and healthcare sectors. • **Providers of critical digital services** like search engines and cloud computing.
Security incidents reporting	• **Take appropriate security measures and report incidents to the national authorities**

Breach notification is the law obligation

- **NIS Directive Art. 14**

  Mandatory incident reporting for operators of essential services
- NIS Directive Art. 16

  Mandatory incident reporting for digital service providers
- GDPR Art. 33

  Mandatory incident reporting for personal data breach
- Telecom Framework Directive Art. 13a

  Mandatory incident reporting in the telecom sector
- eIDAS regulation Art. 19

  Mandatory incident reporting for trust service providers

NIS Directive Art. 14
Security requirements and incident notification

- Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures...
- Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems...
- Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide...
- In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:
  - the number of users affected by the disruption of the essential service
  - the duration of the incident
  - the geographical spread with regard to the area affected by the incident
- On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State...
- After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident

1. SCADA, ICS, OT – terminology and meaning
2. **“Myths” about SCADA security**
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

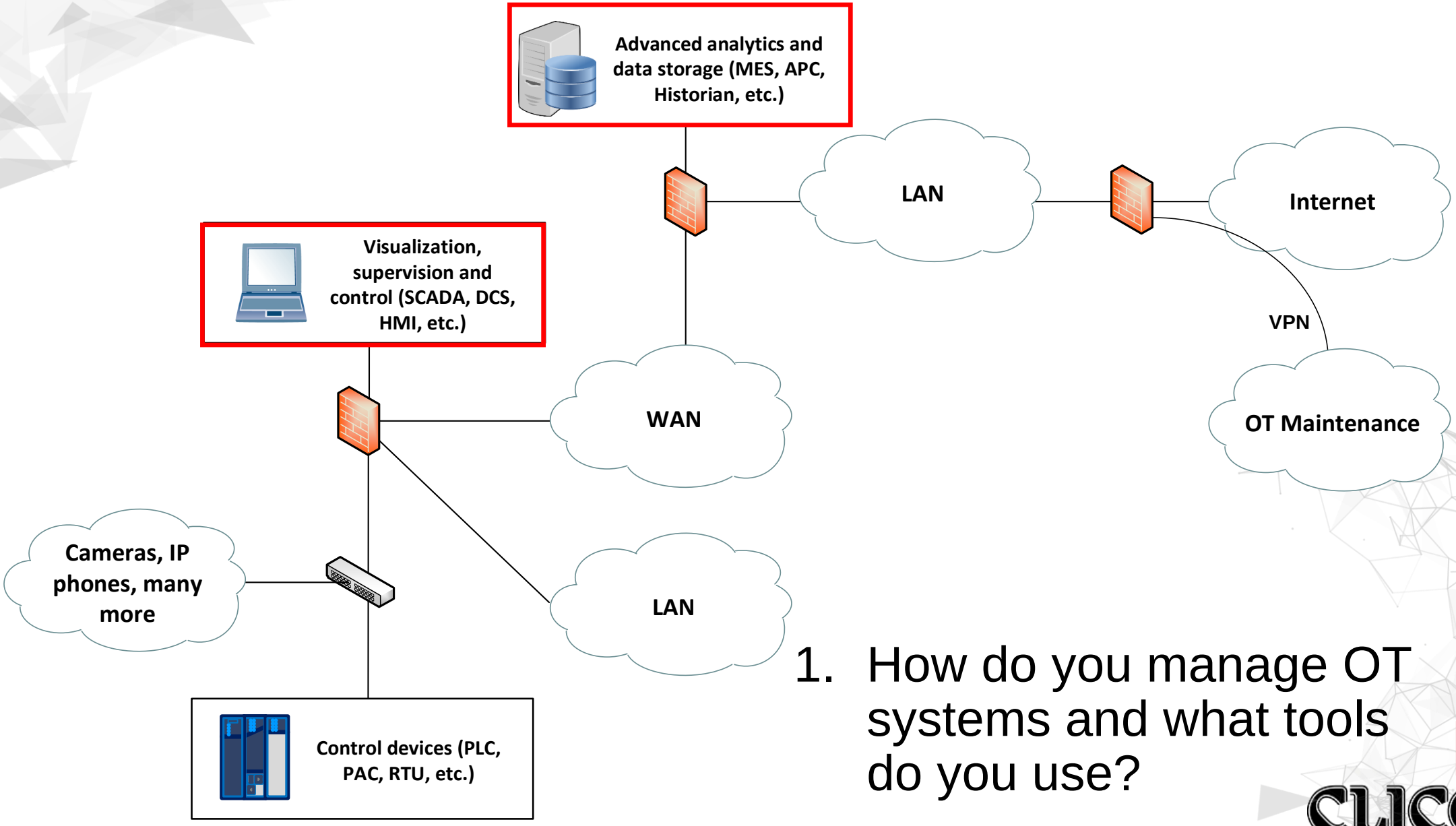
What we hear from OT operators?

1# We do not use SCADA

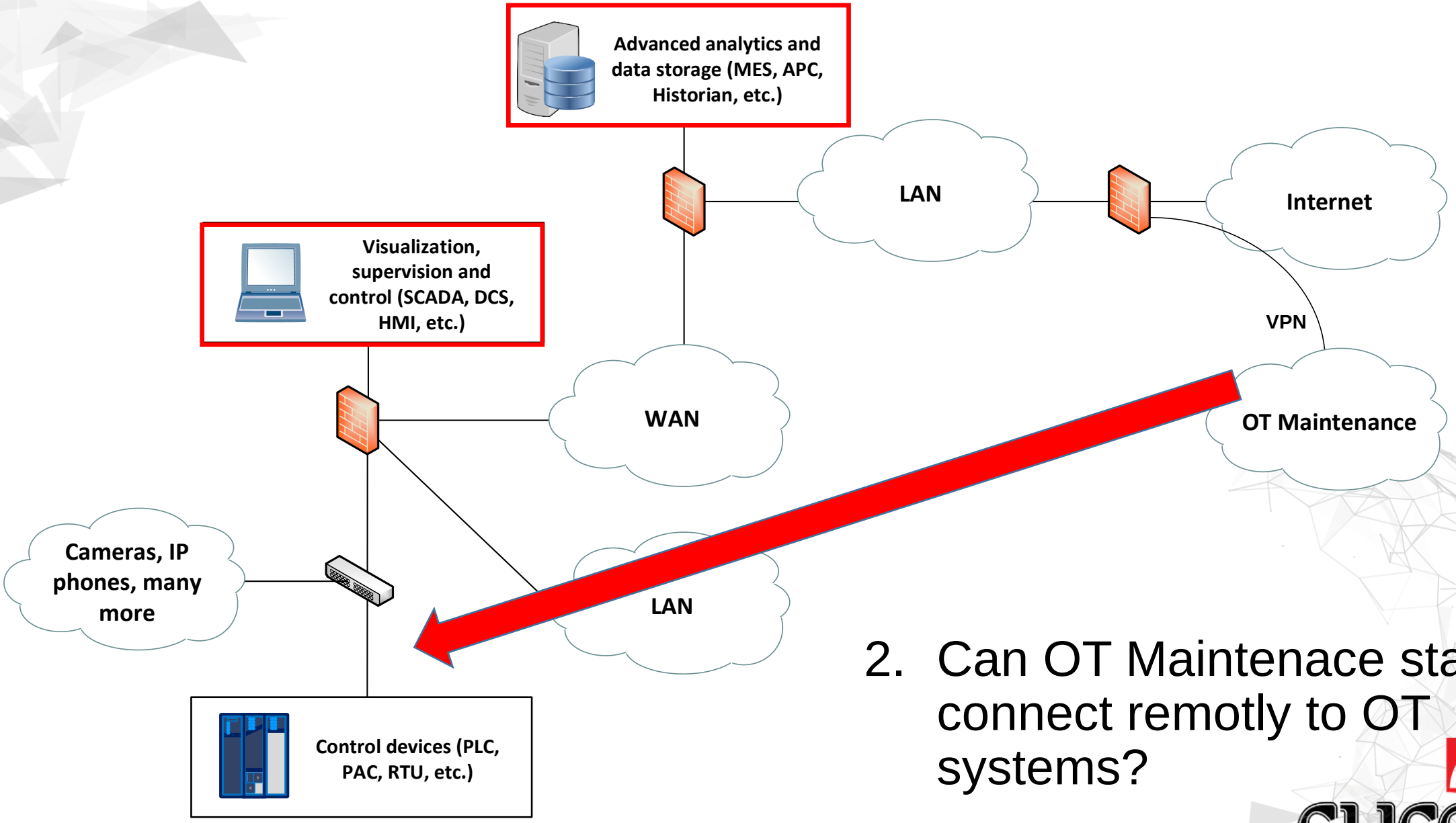
We are safe!

2# Our OT is not connected to the Internet

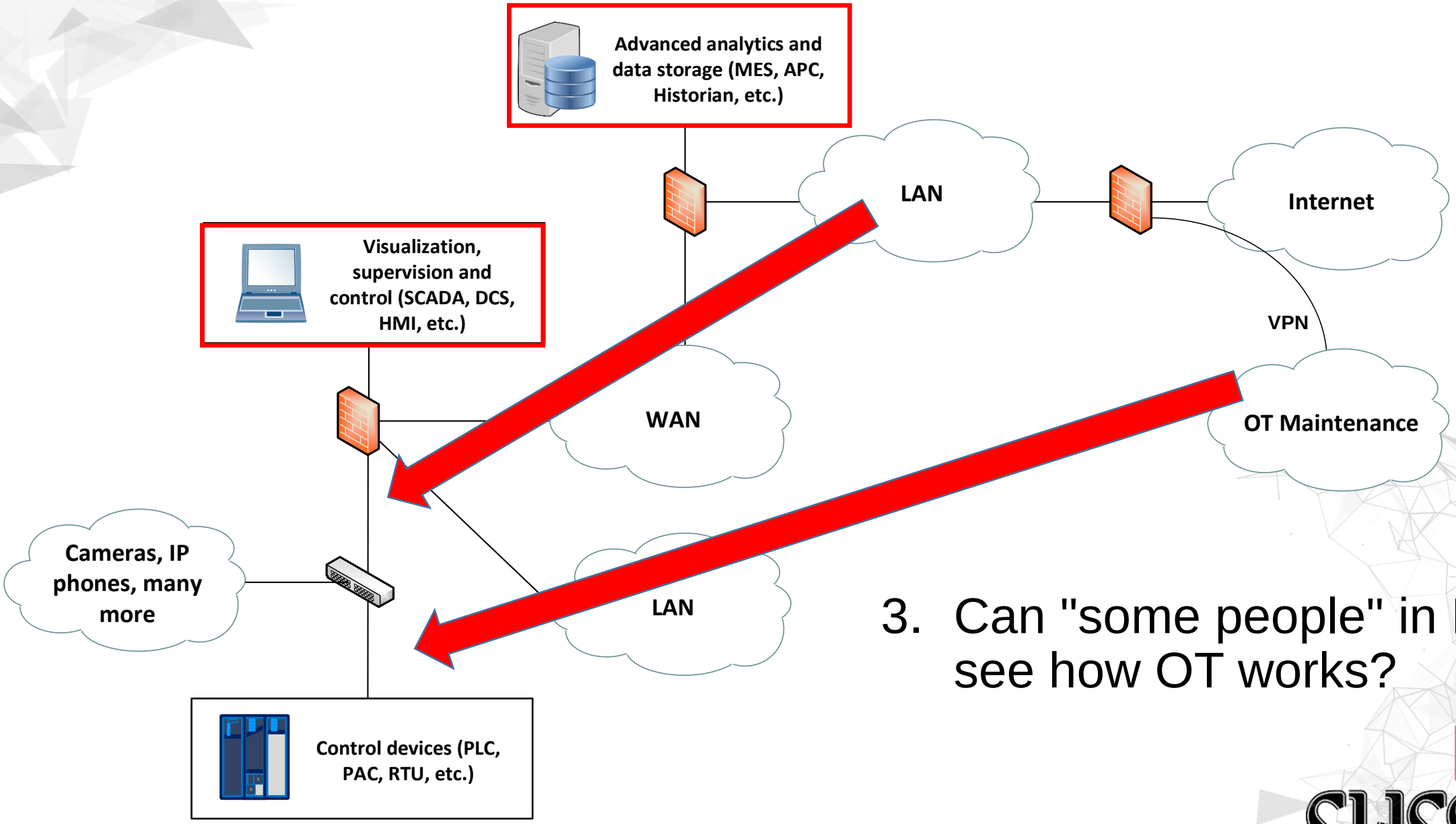
We are safe!



1. How do you manage OT systems and what tools do you use?



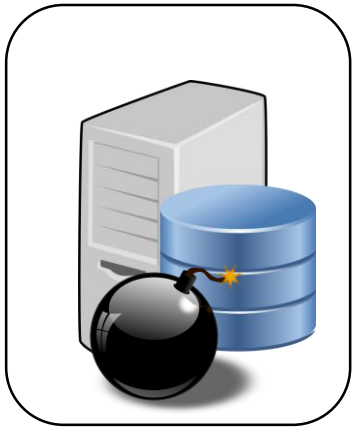
2. Can OT Maintenace staff connect remotly to OT systems?

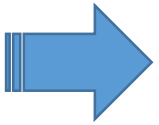


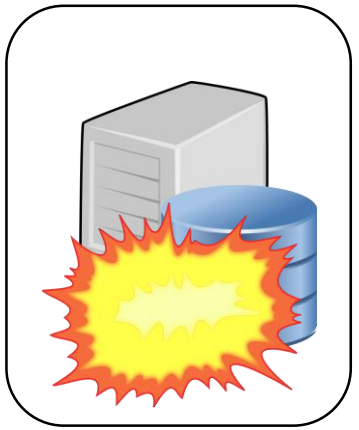
3. Can "some people" in HQ see how OT works?

1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. **Case study of serious SCADA security incident**
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

Example of incident – energy sector, Ukraine 2015







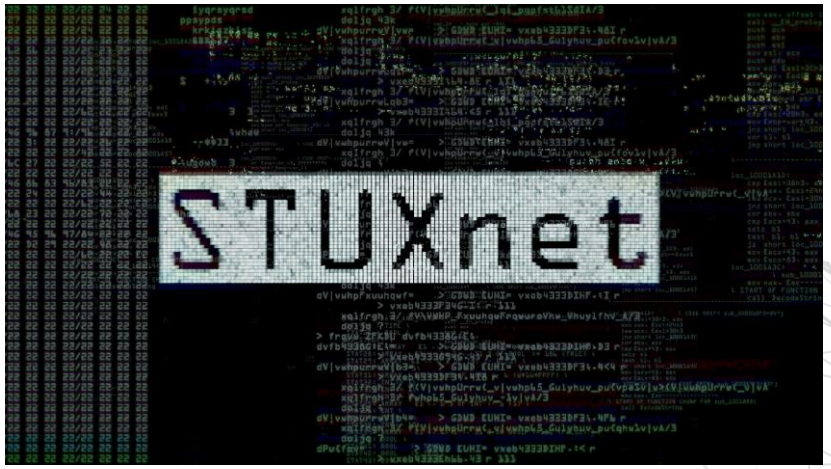
- Social engineering attack (email Phishing)
- The attached in email MS Office doc. installs BlackEnergy 3 malware
- C&C access and recognition of IT environment (+6 months)
- Obtaining data for remote access to ICS systems
- Remote access to ICS systems
- Installation of KillDisk malware
- DoS attack at Call Center

- The attack at the power distribution system (attack by HMI SCADA, resulting in a lack of energy at 225,000 customers)
- False ICS firmware makes difficult the systems recovery
- Turning off the systems backup power supply (UPS)
- Removing the traces of the attack (the removal of logs, destruction / locking systems, etc.)

More information: Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, Electricity Information Sharing and Analysis Center, SANS-ICS, March 18, 2016

Example of incident – nuclear sector, Iran 2012

- Stuxnet is a family of multi-component malware that spreads via removable drives
- Thought to have been in development since at least 2005, Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program. Although neither country has openly admitted responsibility, the worm is believed to be a jointly built American/Israeli cyberweapon.
- To spread, Stuxnet exploits one or more (up to four) vulnerabilities in Microsoft Windows operating systems.
- Once executed on a vulnerable Windows system, the highly sophisticated worm is reportedly designed to search for industrial control systems manufactured by Siemens, generically known as Supervisory Control and Data Acquisition or SCADA systems. Once the targeted SCADA systems are located, the malware will take advantage of, by design, Programmable Logic Controllers (PLCs) and upload its own code to them, reportedly changing the programmed behavior of the PLC



More information: Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, Electricity Information Sharing and Analysis Center, SANS-ICS, March 18, 2016

1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. **Attack methods dangerous for SCADA/OT**
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

OT - Operational Technology

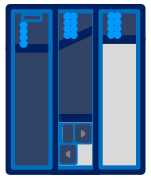
ICS - Industrial Control System = IACS - Industrial Automation and Control System

Advanced analytics and data storage

- MES – Manufacturing Execution System
- APC - Advanced Process Control
- Data Historian

Visualization, supervision and control

- SCADA - Supervisory Control and Data Acquisition
- DCS - Distributive Control System
- HMI - Human Machine Interface



Control devices

- PLC - Programmable Logic Controller
- PAC - Programmable Automation Controller
- RTU - Remote Terminal Unit

Industrial machinery and equipment

No security

Databases — **Exploits**

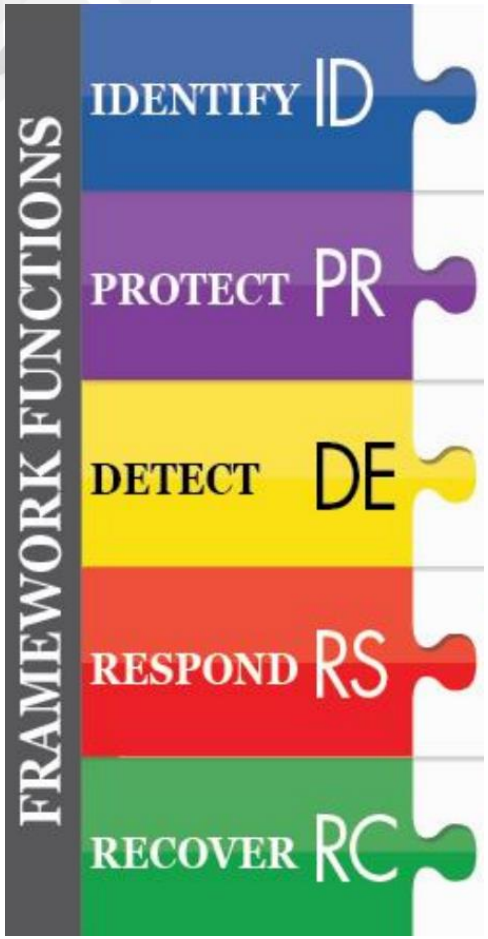
Web — **SQL-I, XSS**

SSH / Remote Access, etc. — **Misuse**

Windows, Linux, etc. — **Malware**

1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. **Fundamental principles of SCADA/OT security**
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

NIST, Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018



Identify – understanding the business context, the resources that support critical functions, and the related cybersecurity risks.
Examples: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Protect – appropriate safeguards to ensure delivery of critical services.
Examples: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect – appropriate activities to identify the occurrence of a cybersecurity event.
Examples: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

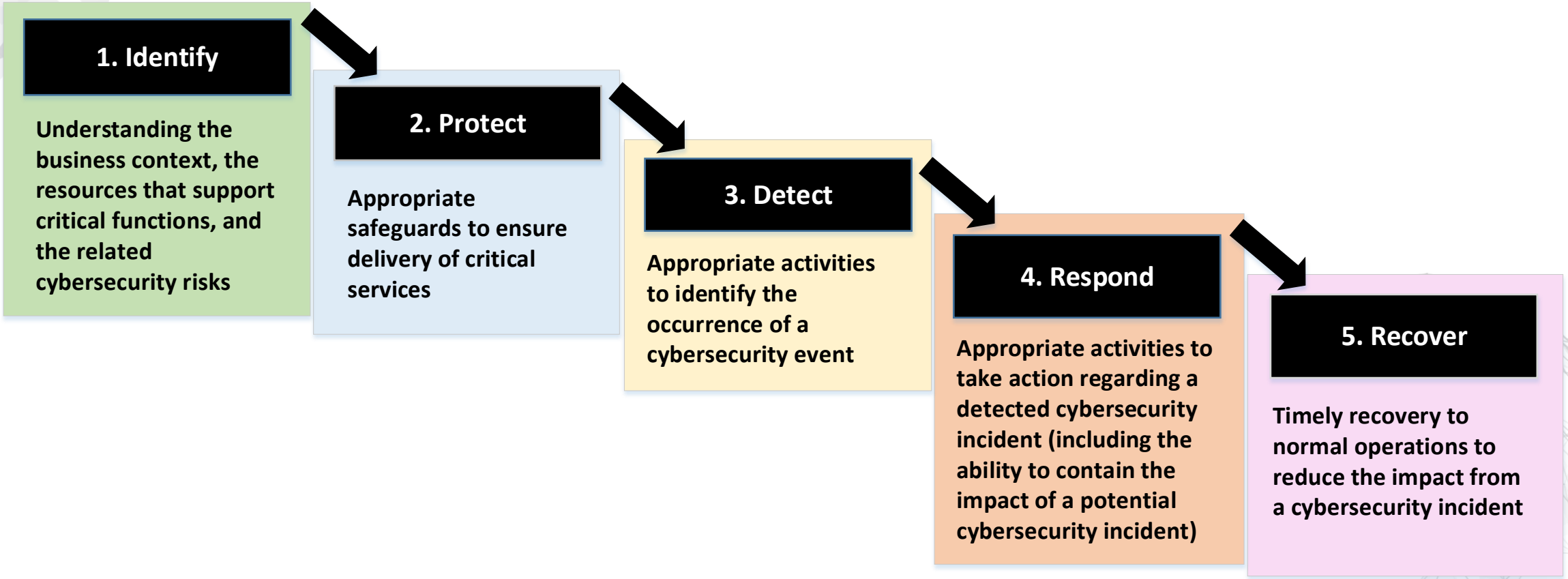
Respond – appropriate activities to take action regarding a detected cybersecurity incident (including the ability to contain the impact of a potential cybersecurity incident).
Examples: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Recover – timely recovery to normal operations to reduce the impact from a cybersecurity incident.
Examples: Recovery Planning; Improvements; and Communications.

CLICO

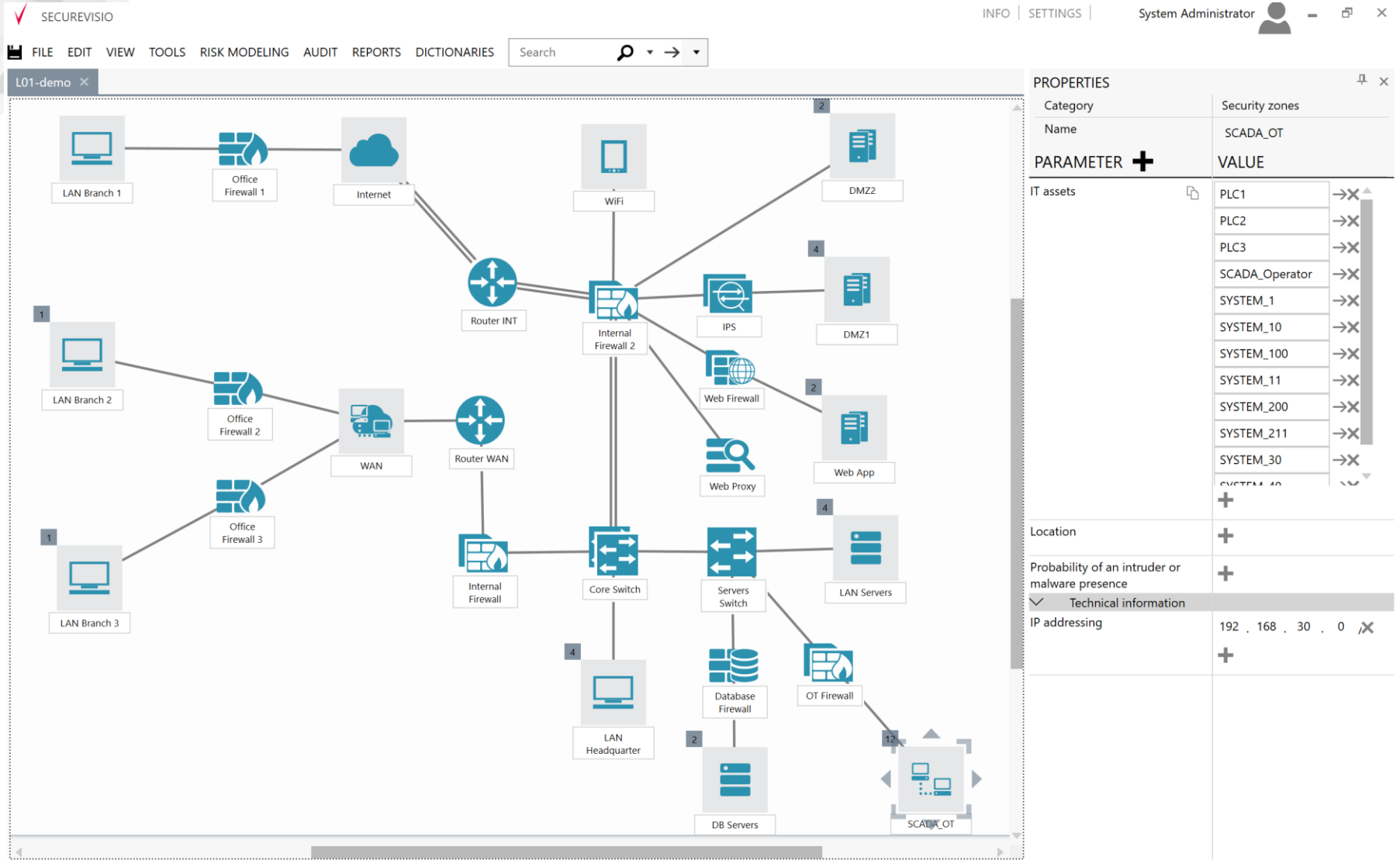
1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. **Good practices in SCADA/OT security projects**
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

NIST, Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018



Risk Management

1. Identify – understanding the business context, the resources that support critical functions, and the related cybersecurity risks



Quick deployment (in 5 steps) of security management tools

SECURE VISIO

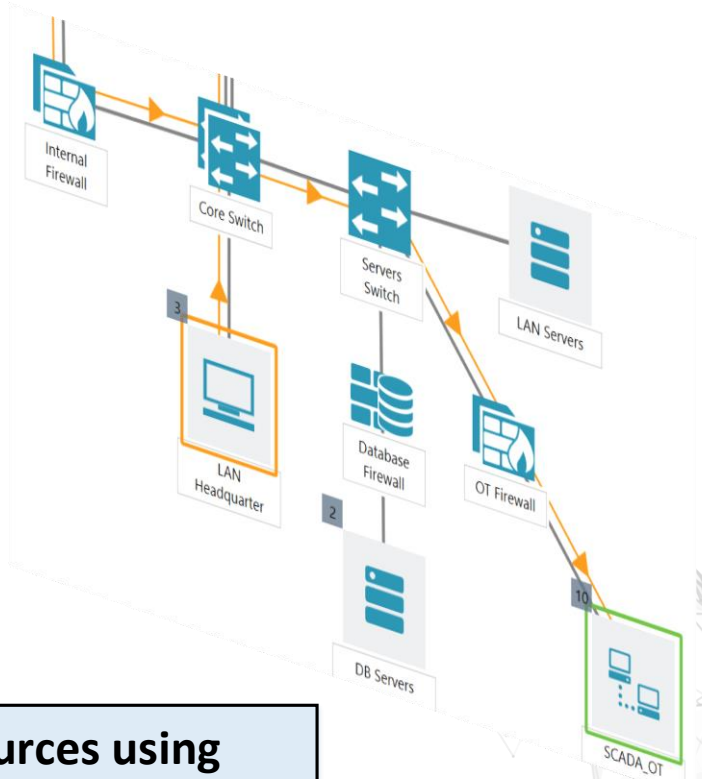
1. Draw network map where IT systems supporting critical services are operating

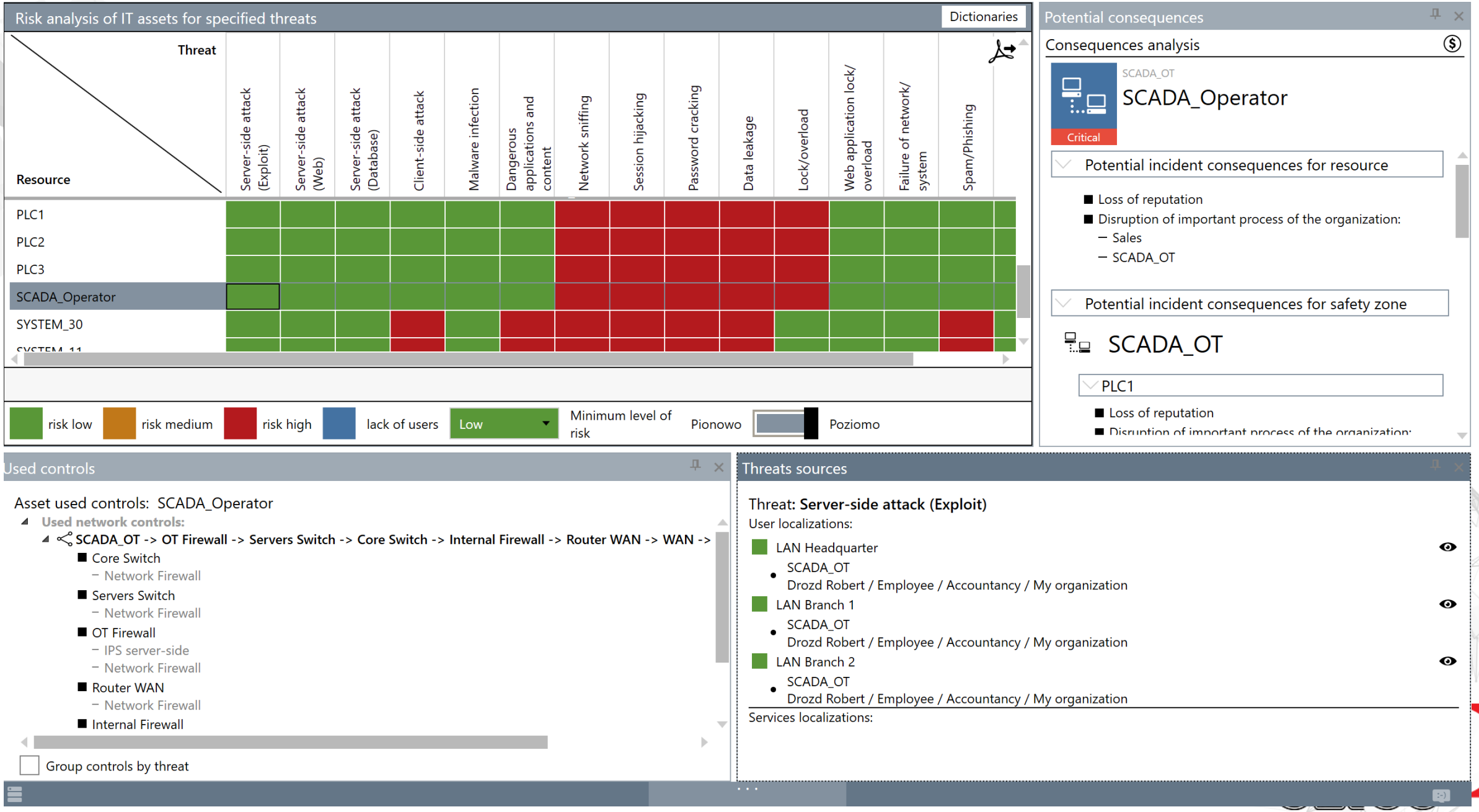
2. Define critical services using Business Process Wizard

3. Connect critical services with IT systems that support them

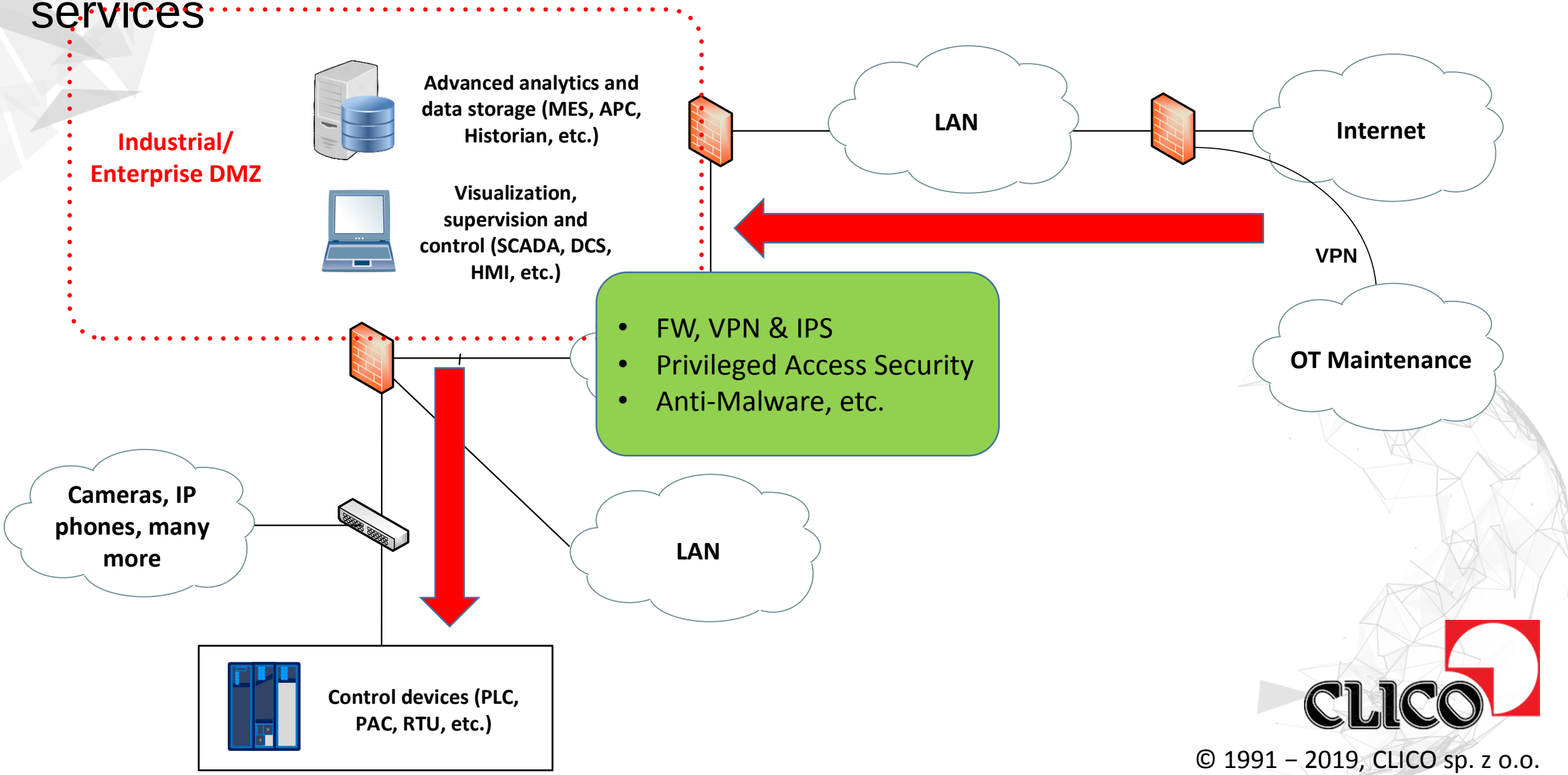
4. Configure alarm sources using Universal Syslog Parser

5. Configure the vulnerability scan schedule





2. Protect – appropriate safeguards to ensure delivery of critical services



3. Detect – appropriate activities to identify the occurrence of a cybersecurity event

4. Respond – appropriate activities to take action regarding a detected cybersecurity incident (including the ability to contain the impact of a potential cybersecurity incident)

5. Recover – timely recovery to normal operations to reduce the impact from a cybersecurity incident

Protection for extreme environments

Protection for extreme environments

- Ruggedized, portalbe appliance
- International Protection Rating: **IP65**

(complete protection against dust and very good protection against water)

- Operating temperature: **-25 to +50°C**

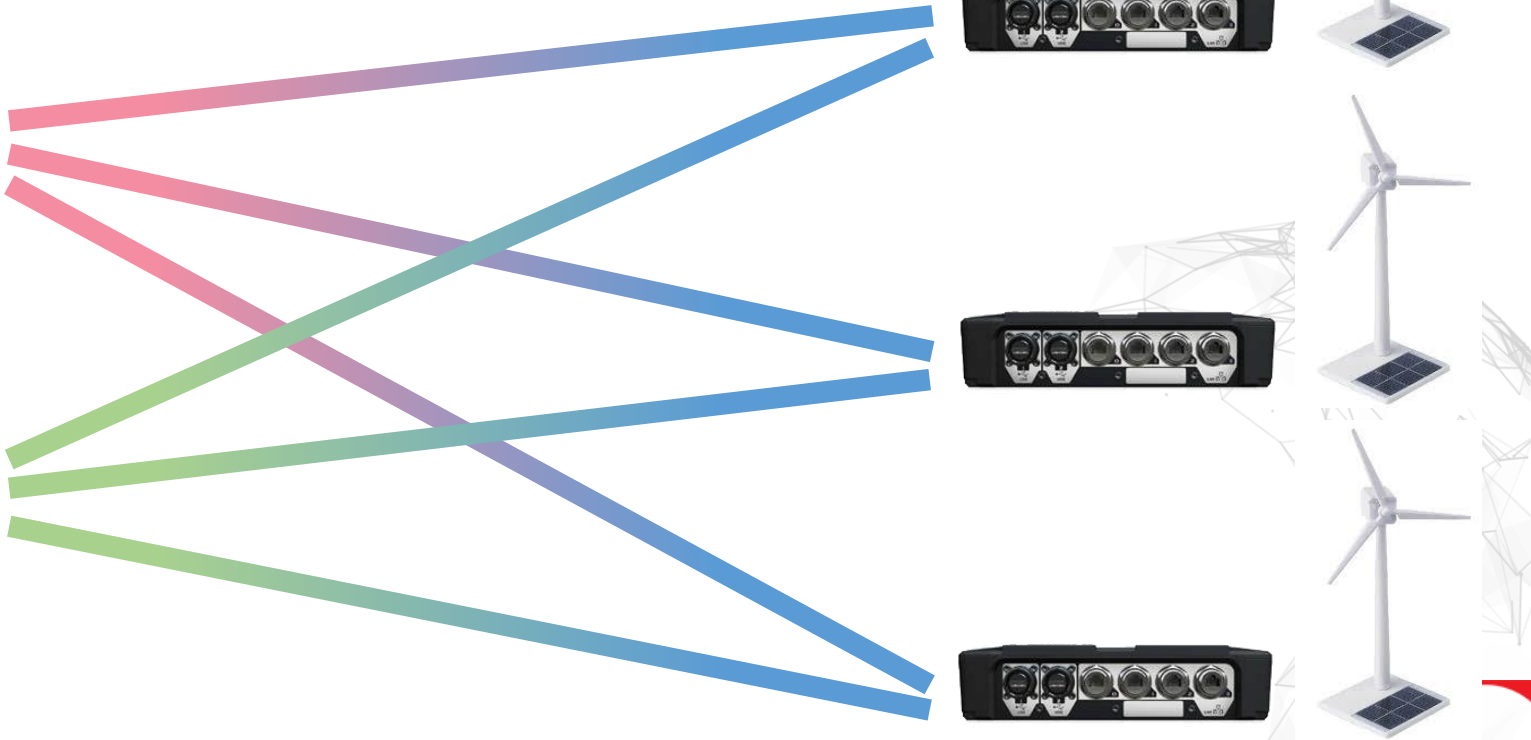
EMC	MIL-STD 461E Requirements: CE102, CS101, CS114, CS115, CS116, RE102, RS103
Environment	IEC 60068-2-1 Aa (Cold) IEC 60068-2-2 Bb (Dry heat) EN 60068-2-30 Dd (Damp heat cyclic) IEC 60529 Casing IP65
Mechanical	IEC 60068-2-6 Fc: Sinusoidal vibration (1.5 G) IEC 60068-2-64 Fc: Random vibration (1.5 G) RMS IEC 60068-2-32 Ed: Drop (75 cm) IEC 60068-2-27 Ea: Shock (50 G) IEC 60068-2-29 Eb: Bump (25 G, 16 ms)

Downtime is NOT an option

FORCEPOINT
POWERED BY Raytheon

ISP A

ISP B

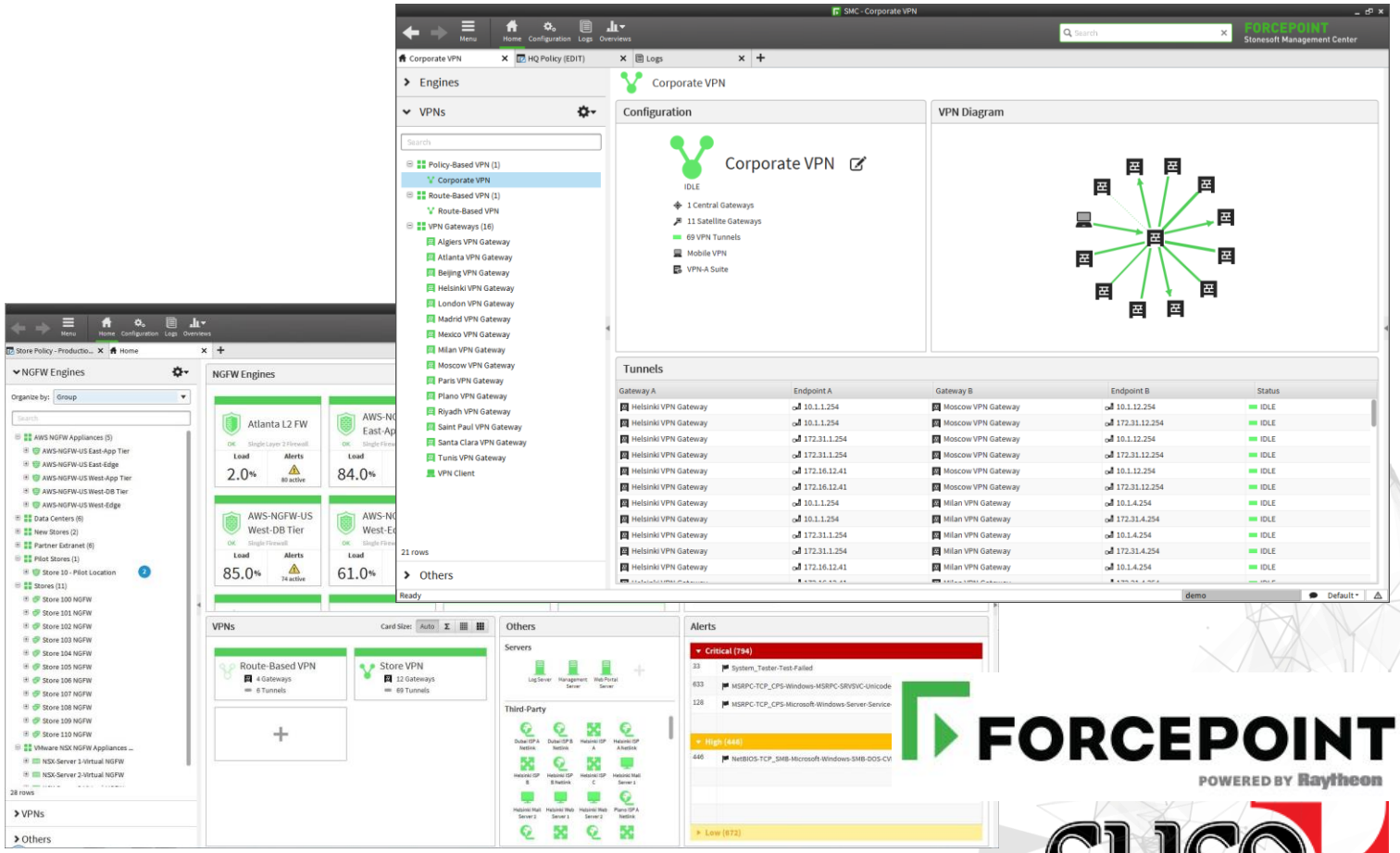


- Multi-Link technology
- VPN Load Balancing (AA / AP)
- Quality of Service over VPN

CLICO

Downtime is NOT an option

- Monitoring
  - NGFW / SMC
  - VPN Tunnels
  - ISP Links
  - Third Party Devices
- Reports
- Overviews



FORCEPOINT
POWERED BY Raytheon

CLICO

Security Comes First

- IPS Builtin. Enabled by Default
- IPS Engine with **Anti-Evasion Defences**
- Software Based IPS. Same Level of Protection Everywhere
- Optimization = Performance
- **Multi-Layer Protocol Normalization**
- **Anomaly Detection**
- Anti-Botnet (Decryption-based detection and message length sequence analysis)
- File Recognition and Filtering
- File Reputation (Forcepoint Reputation Service)
- Local Anti-Virus (McAfee)
- Sandbox (LastLine)
- Web filtering, application control

FORCEPOINT NGFW 3301 Appliance v6.1.2 NEXT GENERATION FIREWALL NSS RECOMMENDED

NGFW
5th Consecutive Time

FORCEPOINT Forcepoint NGIPS 3301 v6.2.1 NEXT GENERATION INTRUSION PREVENTION SYSTEM NSS RECOMMENDED

NGIPS
2nd Consecutive Time

"The security effectiveness of the Forcepoint NGFW 3301 was unsurpassed in the NSS Labs 2017 NGFW test. ***The Forcepoint NGFW should be on every company's short list.***"

Thomas Skybakmoen,
Distinguished Research Director
NSS Labs

FORCEPOINT
POWERED BY Raytheon

Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6 encapsulation, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net ,POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP

CLICO

Protect what values most

SCADA Protocol agents

FORCEPOINT
POWERED BY Raytheon

OPC UA

- ~160 inspection fingerprints
  - ~80 for both implemented stack options
- OPC UA TCP/SC/Binary and SOAP stacks

OPC Classic

- ~40 access control applications
  - Filtering using roughly 40 different applications
  - Uses UUID filtering
  - Opens ports for OPC Classic dynamically

Enables meaningful firewall functionality and control over allowed protocol sub-components

Modbus/TCP

- ~70 Inspection fingerprints
  - Protocol message control
  - Including functionality for non-identified or malformed messages detected

DNP3 over TCP/UDP

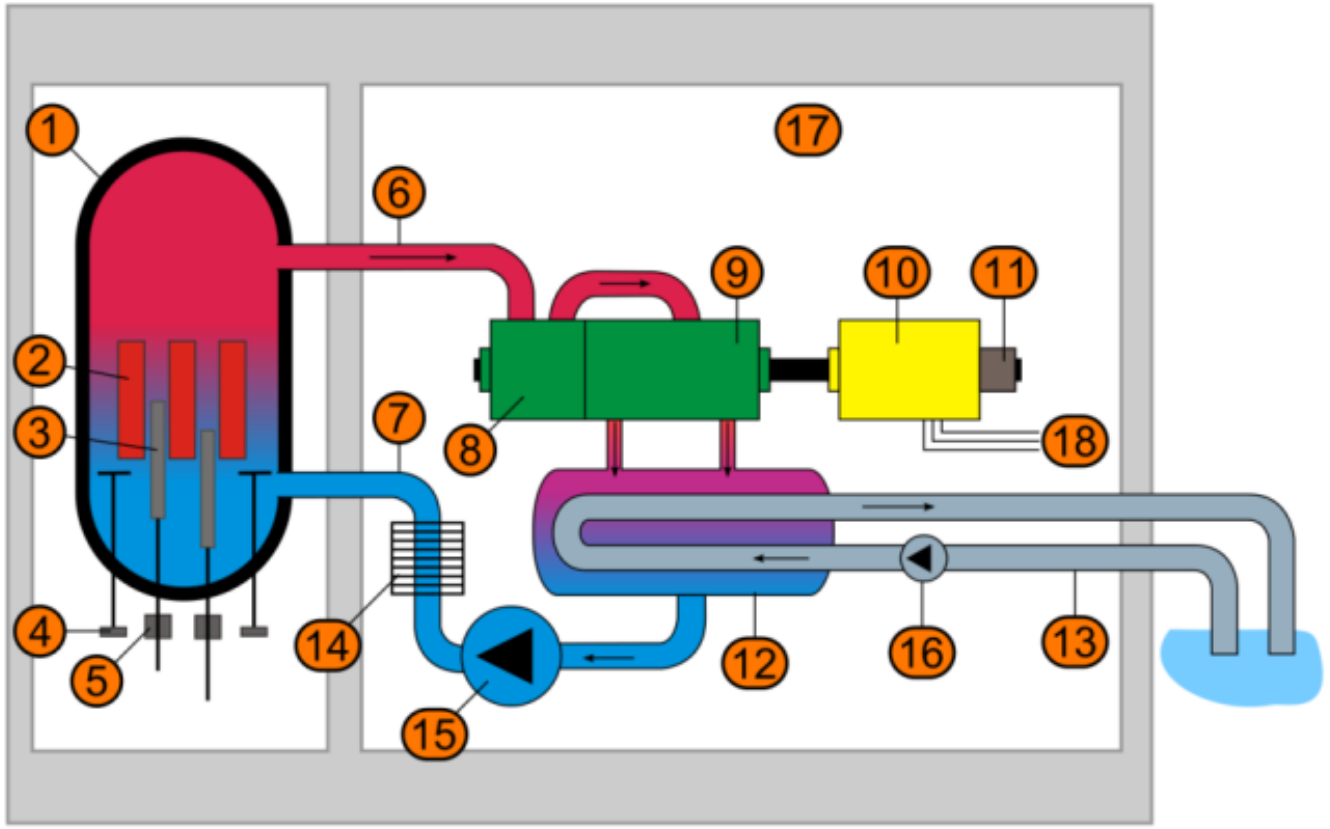
- ~80 inspection fingerprints
  - Protocol message control
  - Including functionality for non-identified or malformed messages detected

Protect what values most

FORCEPOINT
POWERED BY Raytheon

Protocol Control

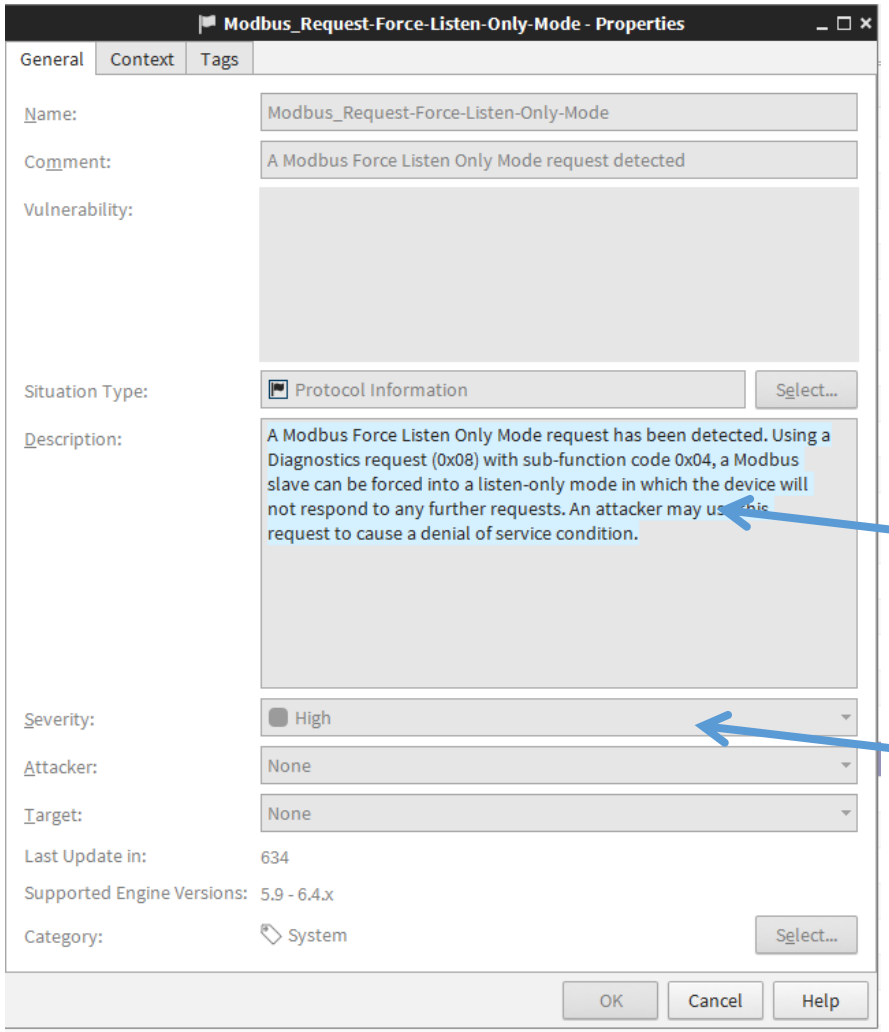
- Understanding traffic
- Read / Write
- Diagnostics
- Error detection
- Checksum
- State tracking



CLICO

Modbus_Read-FIFO-Queue-Request	*Do Not Inspect*	*None*		
Modbus_Read-FIFO-Queue-Response	Permit	Stored		@2097377.0
Modbus_Read-File-Record-Error-Response	Permit	Stored		@2097376.0
Modbus_Read-File-Record-Request	Permit	Transient		@2097375.0
Modbus_Read-File-Record-Response	Permit	Stored		@2097374.0
Modbus_Read-Holding-Registers-Error-Response	Permit	Stored		@2097373.0
Modbus_Read-Holding-Registers-Request	Permit	Stored		@2097372.0
Modbus_Read-Holding-Registers-Response	Permit	Stored		@2097371.0
Modbus_Read-Input-Registers-Error-Response	Permit	Stored		@2097370.0
Modbus_Read-Input-Registers-Request	Permit	Stored		@2097369.0
Modbus_Read-Input-Registers-Response	Permit	Stored		@2097378.0
Modbus_Read/Write-Multiple-Registers-Error-Response	Permit	Stored		@2097382.0
Modbus_Read/Write-Multiple-Registers-Request	Permit	Stored		@2097379.0
Modbus_Read/Write-Multiple-Registers-Response	Permit	Stored		@2097381.0
Modbus_Report-Slave-Id-Error-Response	Permit	Stored		@2097380.0
Modbus_Report-Slave-Id-Request	Permit	Stored		@2097383.0
Modbus_Report-Slave-Id-Response	Permit	Stored		@2097384.0
Modbus_Request-Clear-Counters-And-Diagnostics-Register	Permit	Stored		@2097385.0
Modbus_Request-Force-Listen-Only-Mode	Terminate	Essential		@2097386.0
Modbus_Request-Reserved-Function-Code	Permit	Stored		@2097387.0
Modbus_Request-Restart-Communications-Option	Terminate	Essential		@2097388.0
Modbus_Request-User-Defined-Function-Code	Permit	Stored		@2097389.0
Modbus_Response-Reserved-Function-Code	Permit	Stored		@2097390.0
Modbus_Response-User-Defined-Function-Code	Permit	Stored		@2097391.0

Protect what values most

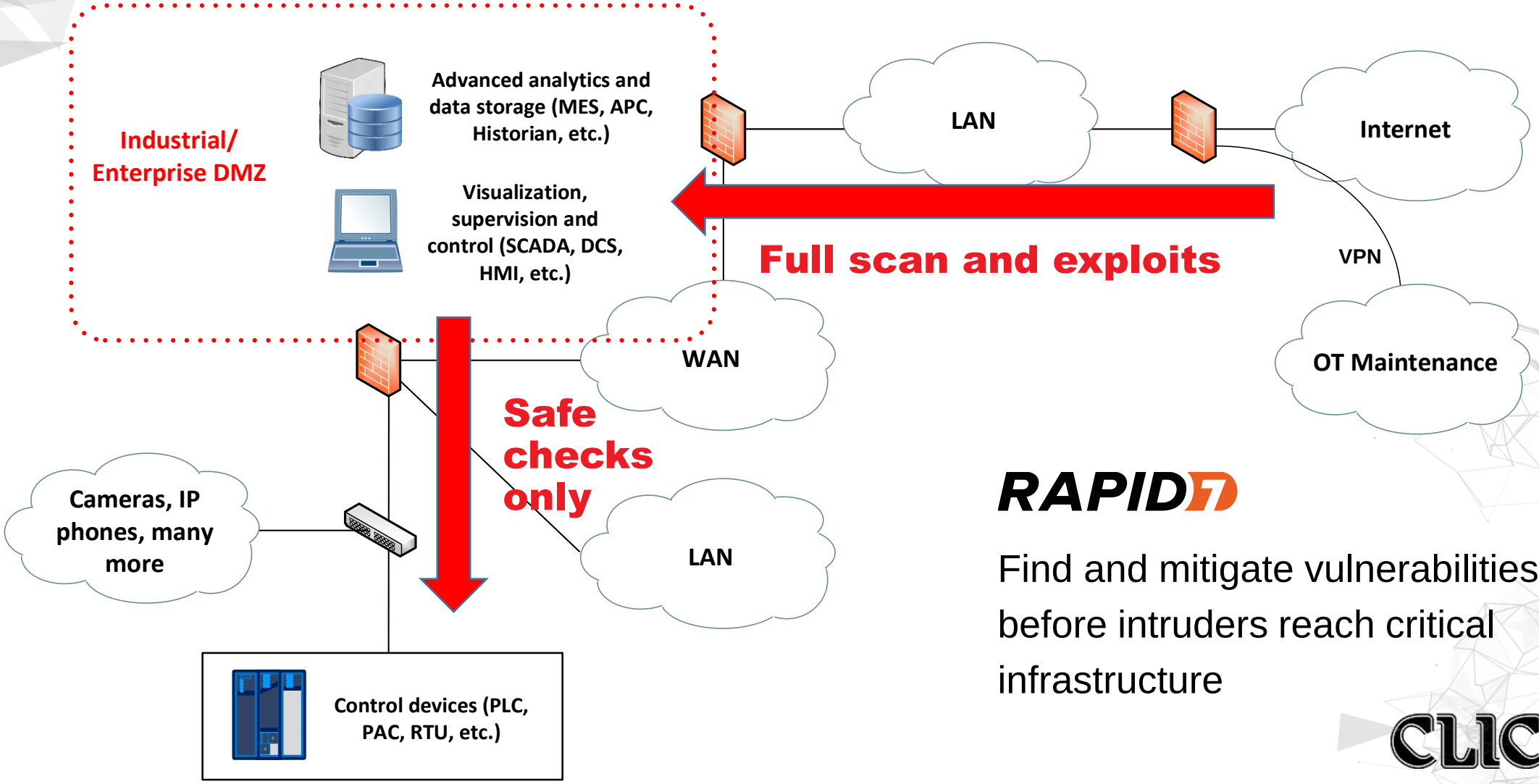


Description

Severity

1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. **Vulnerability management and validation in SCADA/OT**
8. Dynamic Data Protection(DDP)
9. Controlling OT and IT connection of SCADA systems

Reduce attack surface with the networks segmentation and vulnerabilities mitigation



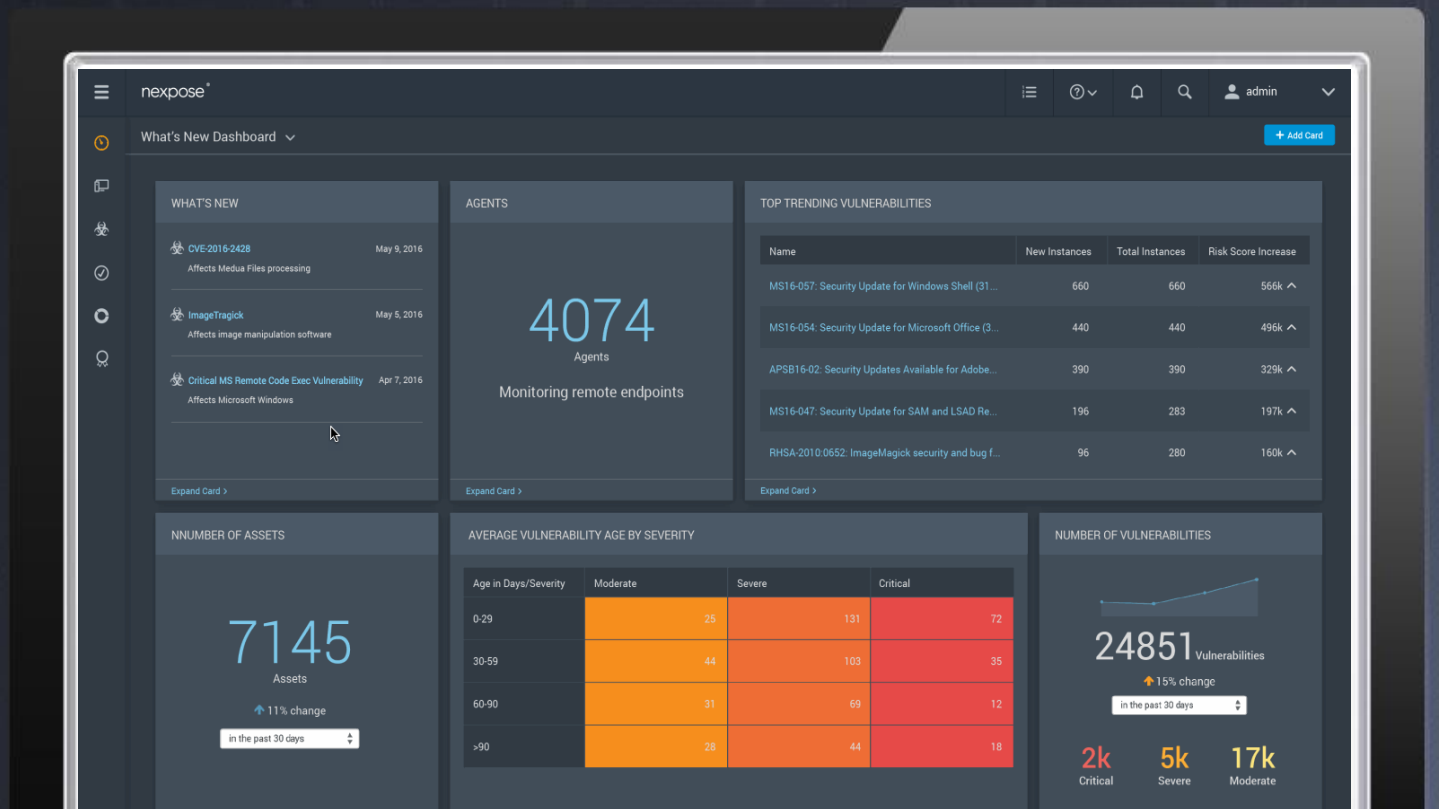
RAPID7

Find and mitigate vulnerabilities before intruders reach critical infrastructure

CLICO

nexpose®

Vulnerability Management



COLLECT

Live Monitoring, Adaptive Security, and advanced collection provides coverage without waiting for scans or drowning in obtuse data

PRIORITIZE

Vulnerability prioritization moves you beyond the paralysis of CVSS-only scores

REMEDIATE

Streamlined Remediation Workflow makes IT your best friend and tracks progress in real-time

CLICO

VA scan templates

Full audit

This full network audit of all systems uses only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. The system scans only default ports and disables policy checking, which makes scans faster than with the Exhaustive scan. Also, This template does not check for potential vulnerabilities.

Use this template to run a thorough vulnerability scan

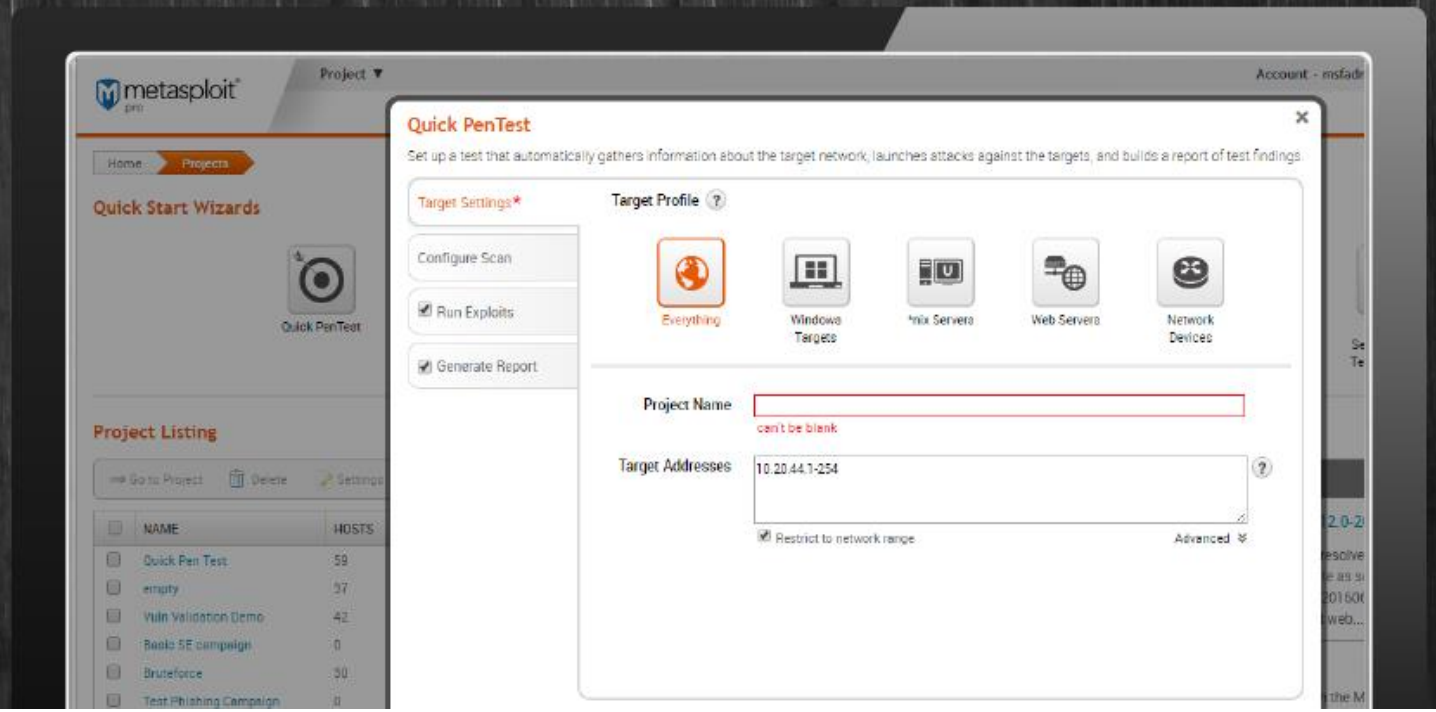
SCADA audit

This is a “polite,” or less aggressive, network audit of sensitive Supervisory Control And Data Acquisition (SCADA) systems, using only safe checks. Packet block delays have been increased; time between sent packets has been increased; protocol handshaking has been disabled; and simultaneous network access to assets has been restricted.

Use this template to scan SCADA systems

metasploit®

Penetration Testing



COLLECT

Gather together the collective knowledge of a global security community to test your network and find your holes

PRIORITIZE

Test and harden your people, your processes, and your technology in order of potential impact

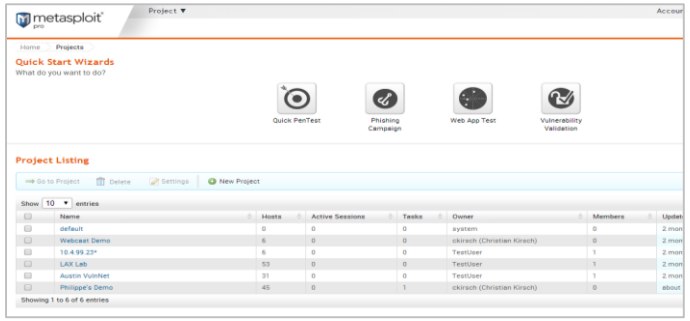
REMEDIATE

Test your security program to identify and more quickly fix exposures

CLICO

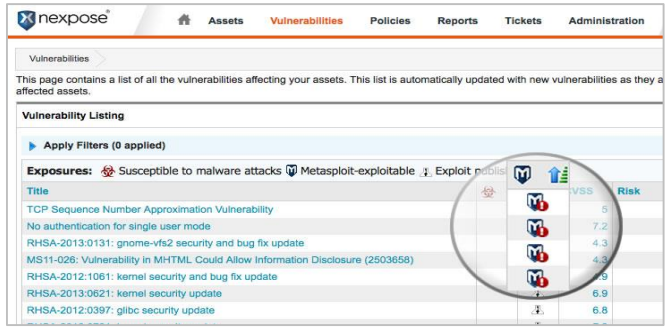
Key points to focus on

Penetration Testing



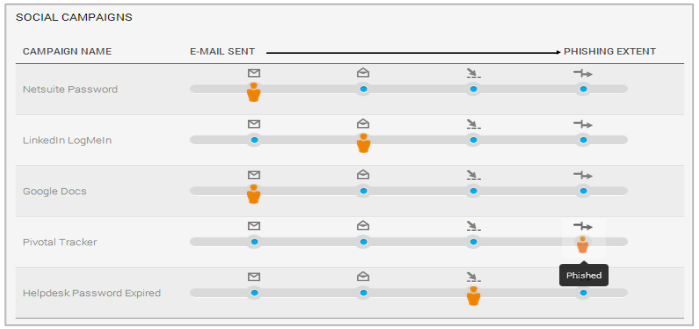
- Simulate a real-world attack to test your defenses

Vulnerability Validation



- Validate vulnerabilities to demonstrate risk
- Close-loop integration with Nexpose for remediation

Phishing Simulation



- Validate vulnerabilities of „the weakest point” by social-tests

Automated Vulnerability Validation

- Nexpose makes it easy to identify and prioritize vulnerabilities
- After remediation, use Metasploit to simulate an attack and verify the effectiveness of your controls

Vul. assessment

Vul. validation

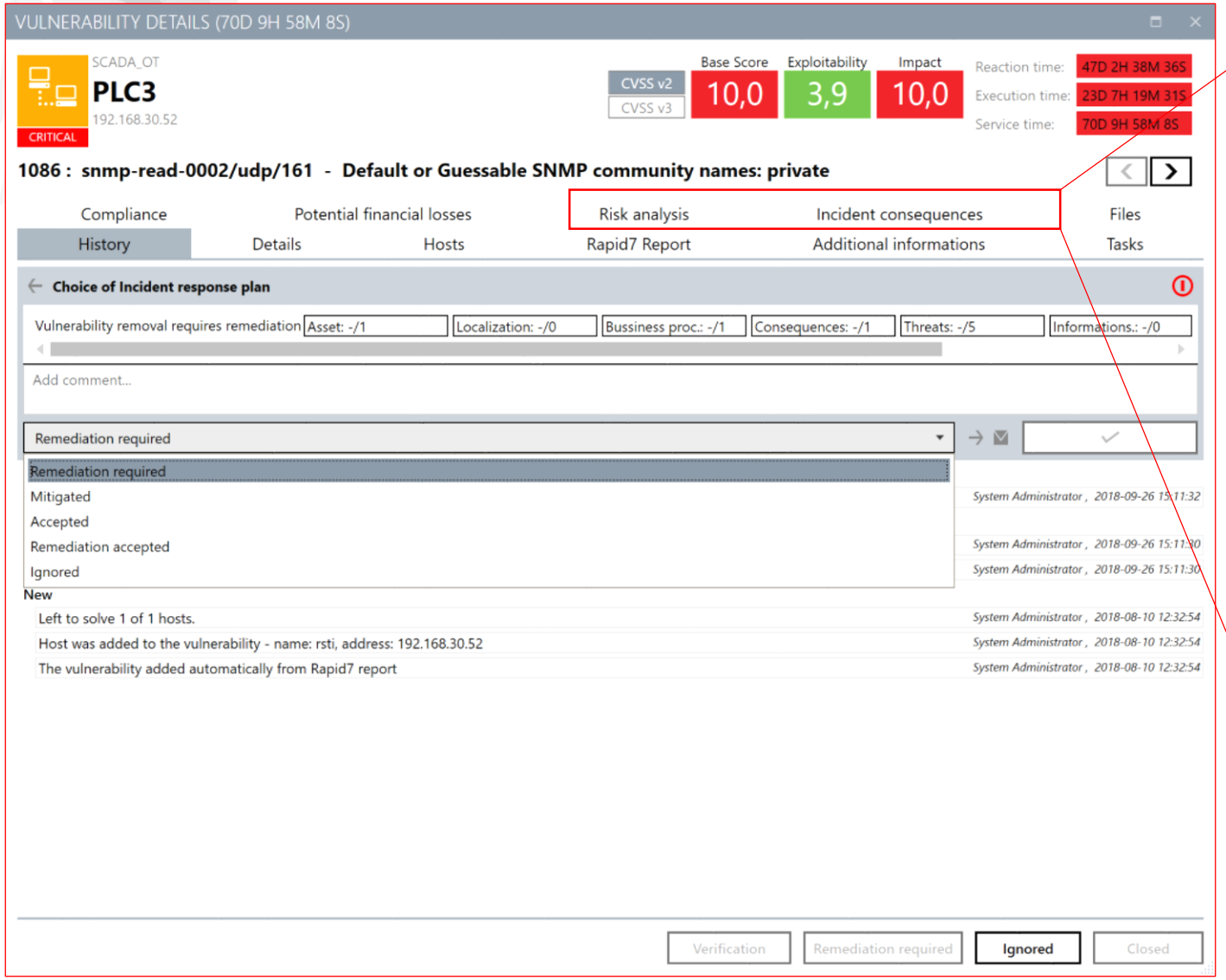
nexpose®

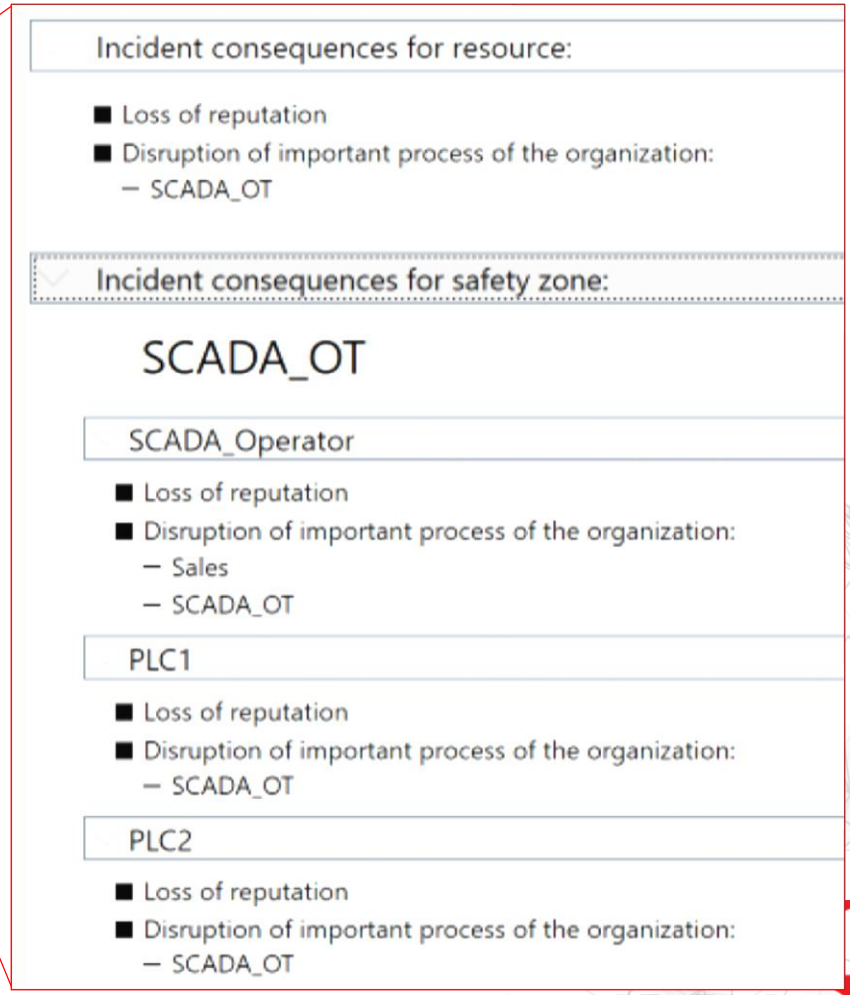
Vulnerability Management & Configuration Assessment

metasploit®

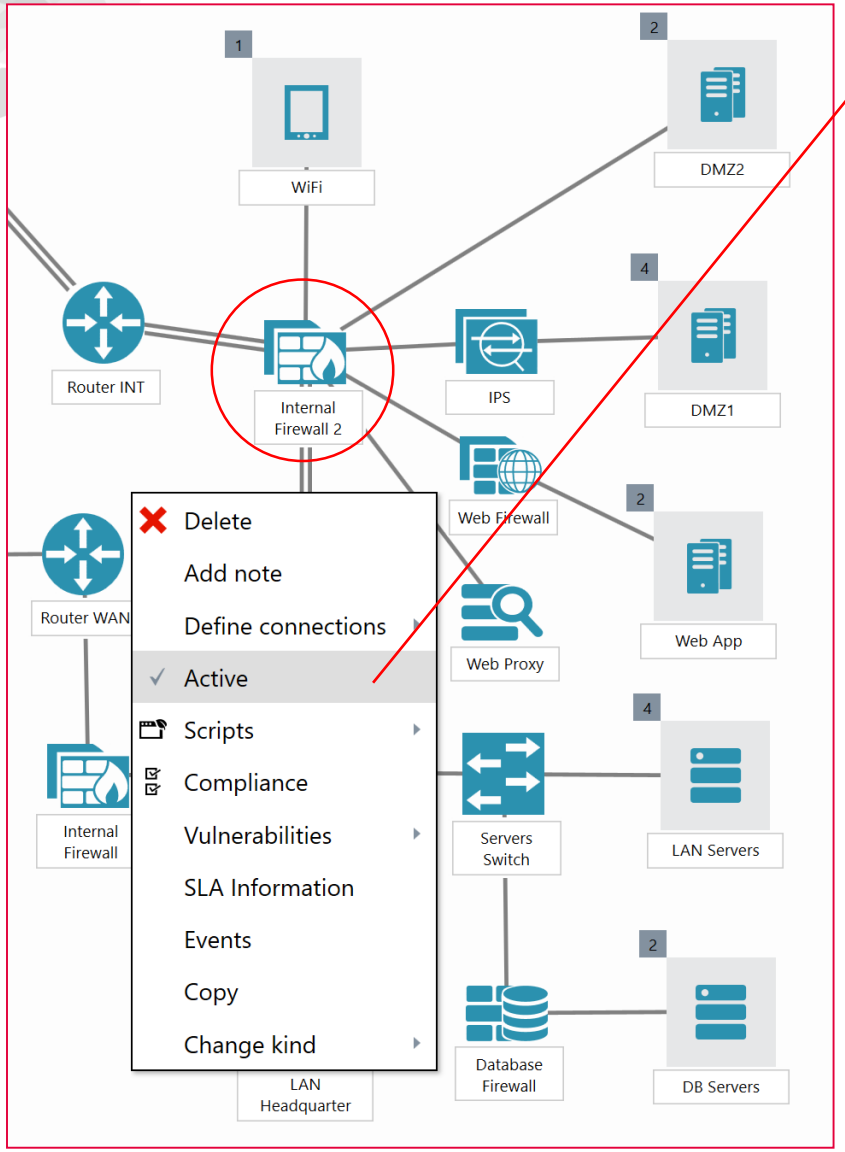
Penetration Testing & Threat Validation

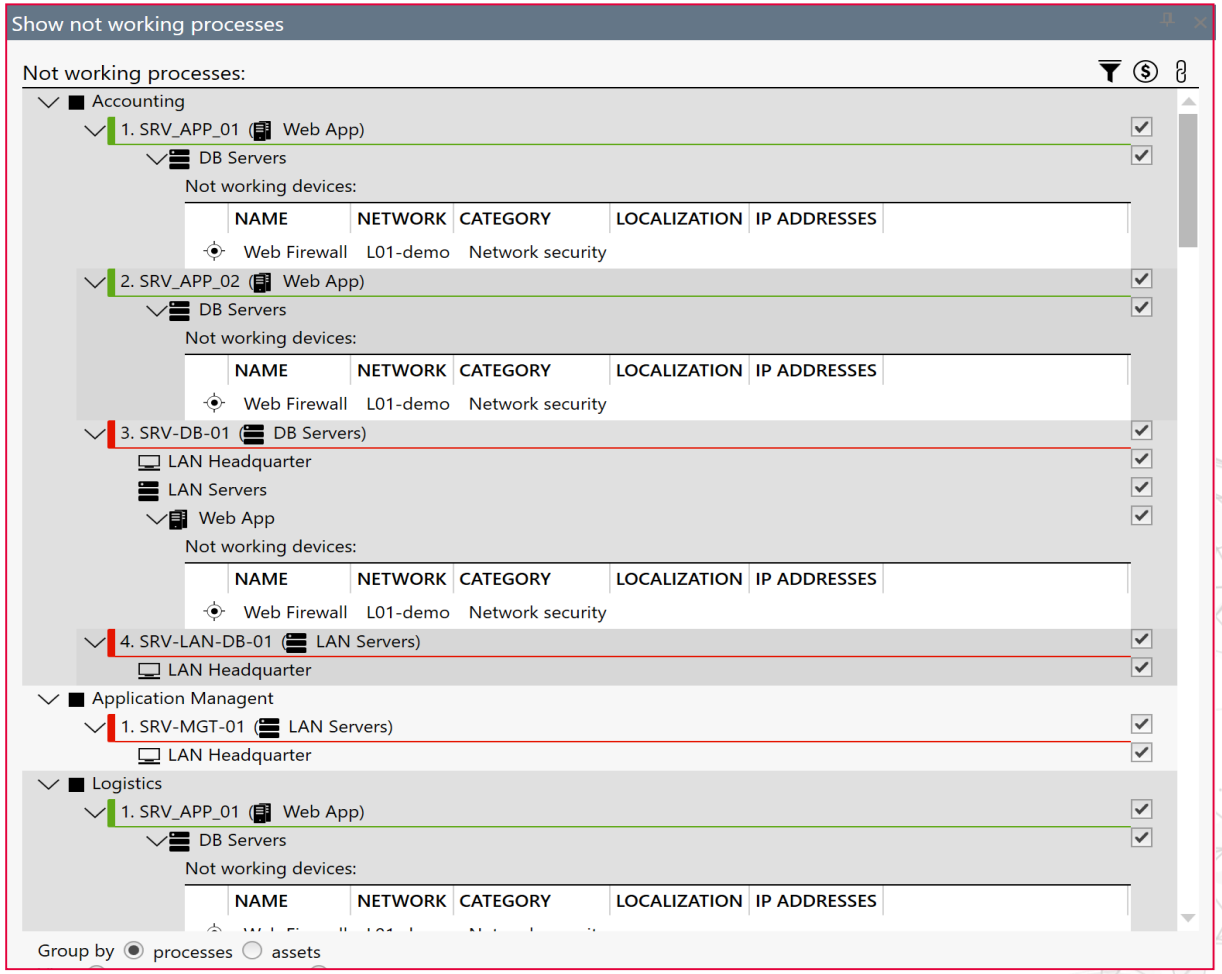
Automate vulnerability management and business prioritization (BIA)





Simulation of device failures with business damage analysis





1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. **Dynamic Data Protection(DDP)**
9. Controlling OT and IT connection of SCADA systems

DLP: Data Leak Prevention

1. Data protection by identifying, monitoring and enforcing DLP policies for data:
   - ✓ **In motion,** when they are sent to internal or external recipient
   - ✓ **In use**, when they are processed on the user workstation
   - ✓ **At rest**, stored in corporate repositories (shares, databases, etc).
2. Mature DLP systems are aware not only of the **content**, but also the **context** in which data is used and communicated.

Forcepoint DLP system components

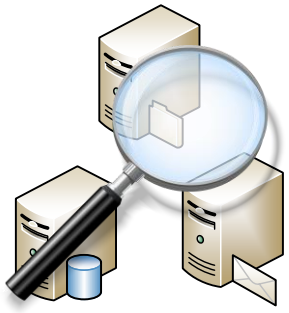
Protect data on network level, data in motion

DLP Network

Protect data on endpoint, in motion, use and at rest

DLP Endpoint

Data discovery, data at rest

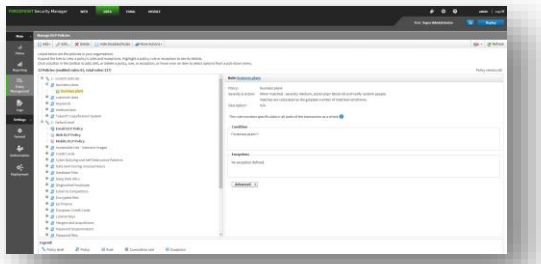


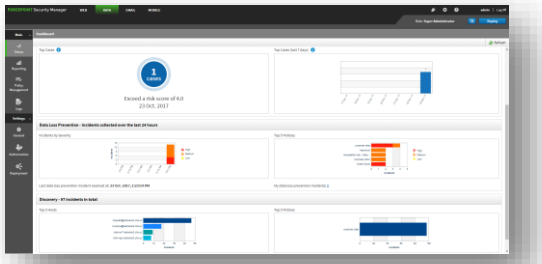
DLP Discover

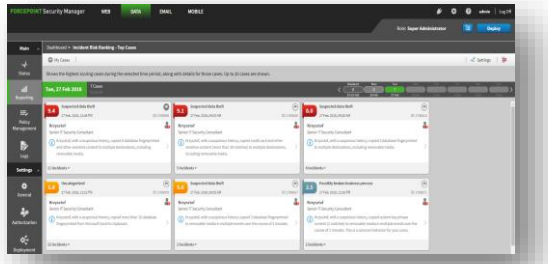
Data in cloud, data at rest, in motion or in use across popular enterprise cloud applications

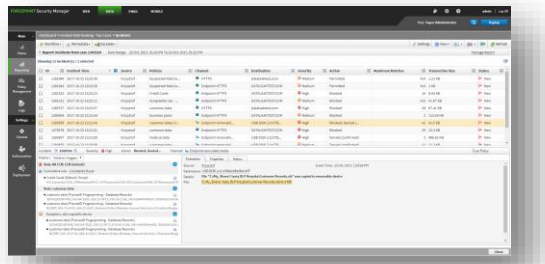
DLP Cloud Applications

Central management and reporting from one console









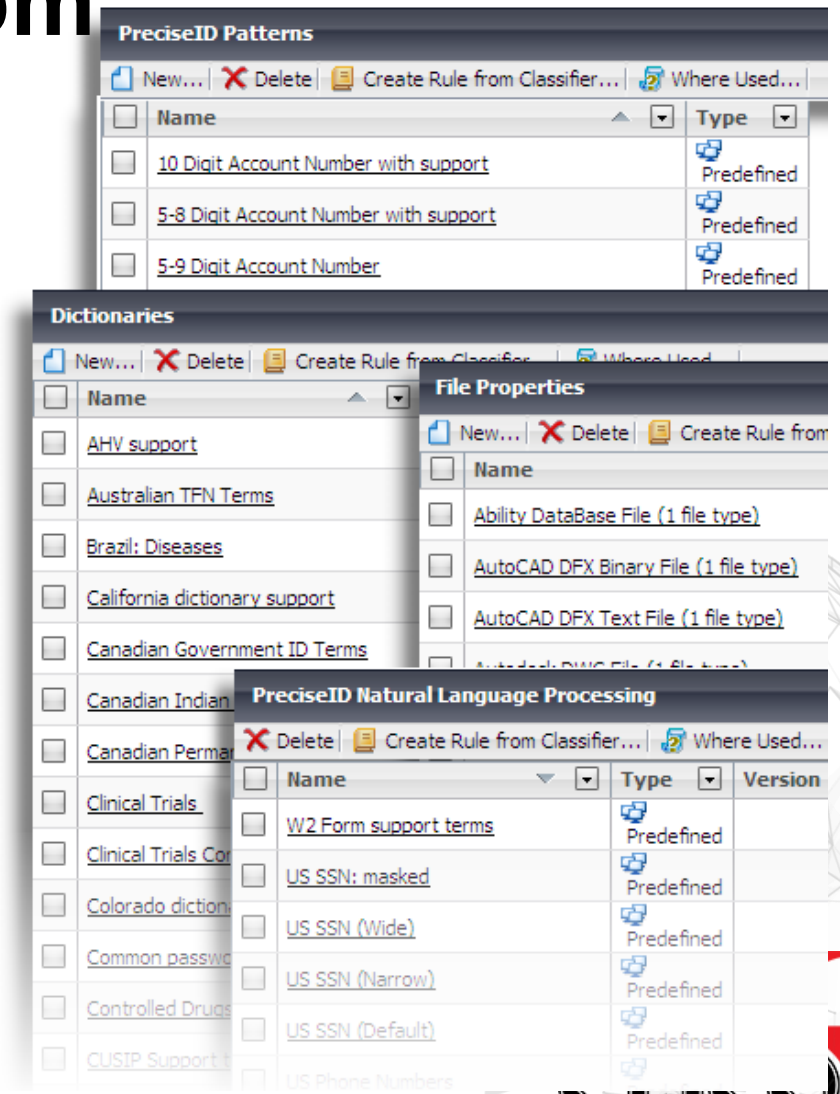
Classifiers - built-in and custom

DLP Compliance

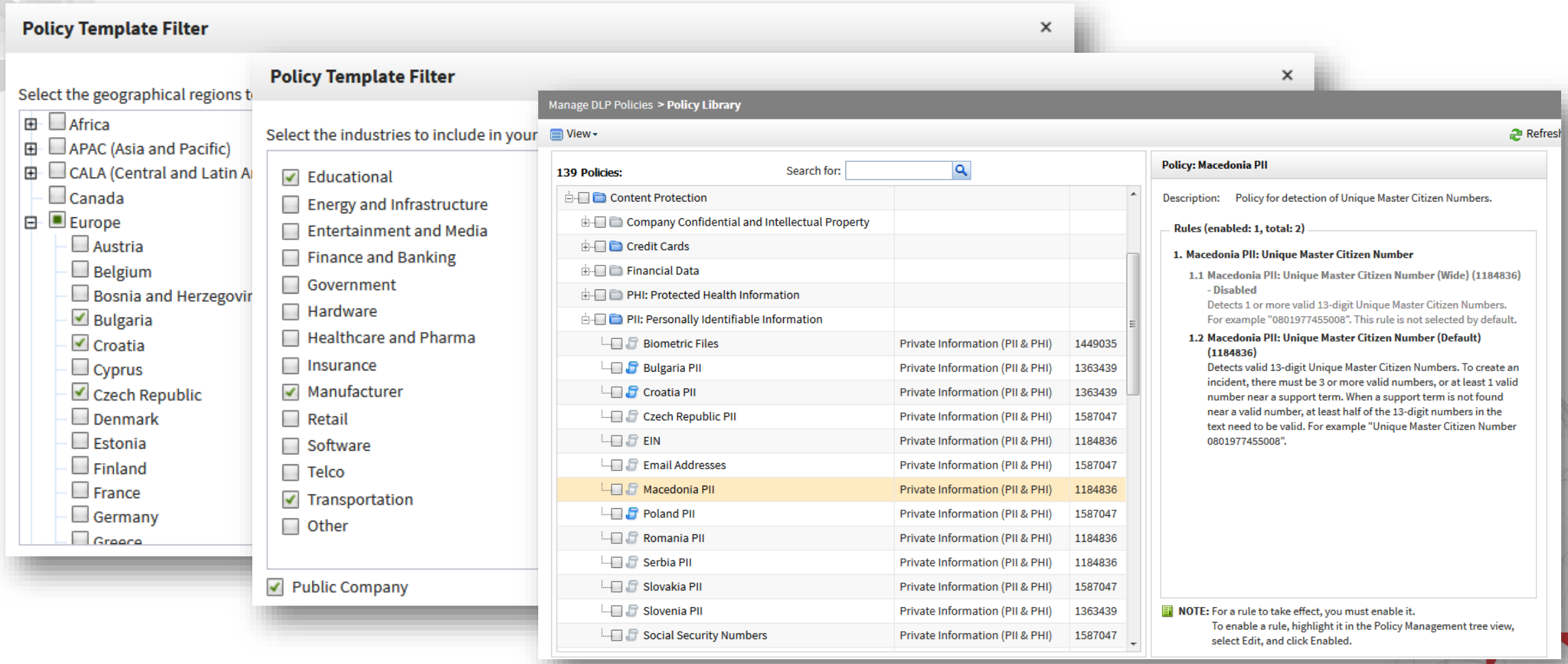
- Built-in classifiers
  - Keywords, dictionaries
  - Regular expressions
  - File properties
  - NLP – Natural Language Processing

- Custom classifiers, including
  - PreciseID fingerprints and
  - Machine Learning

DLP IP Protection



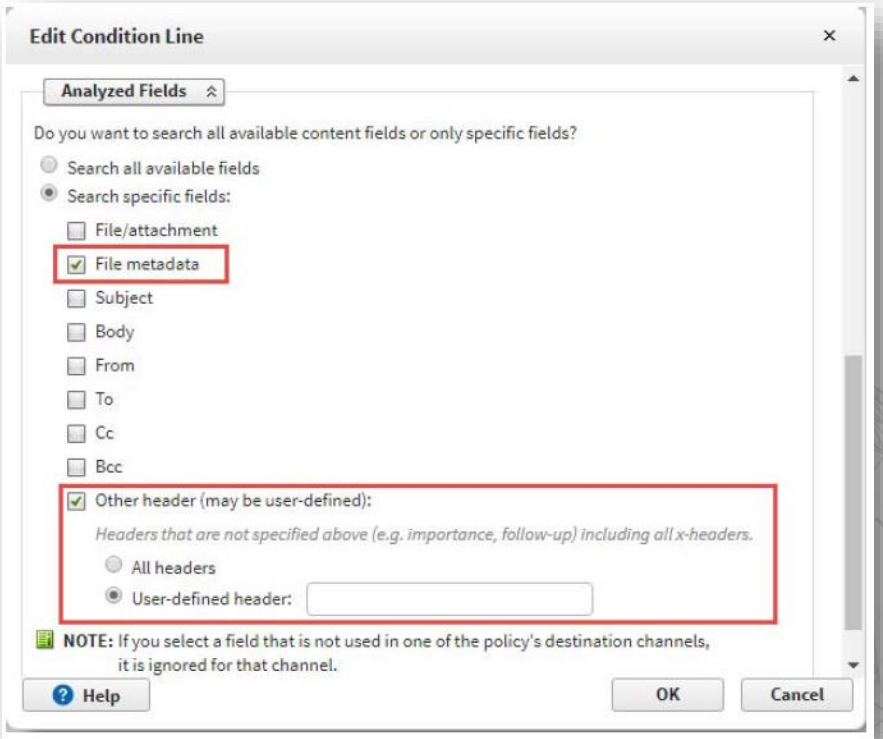
Built-in policy wizard for data protection

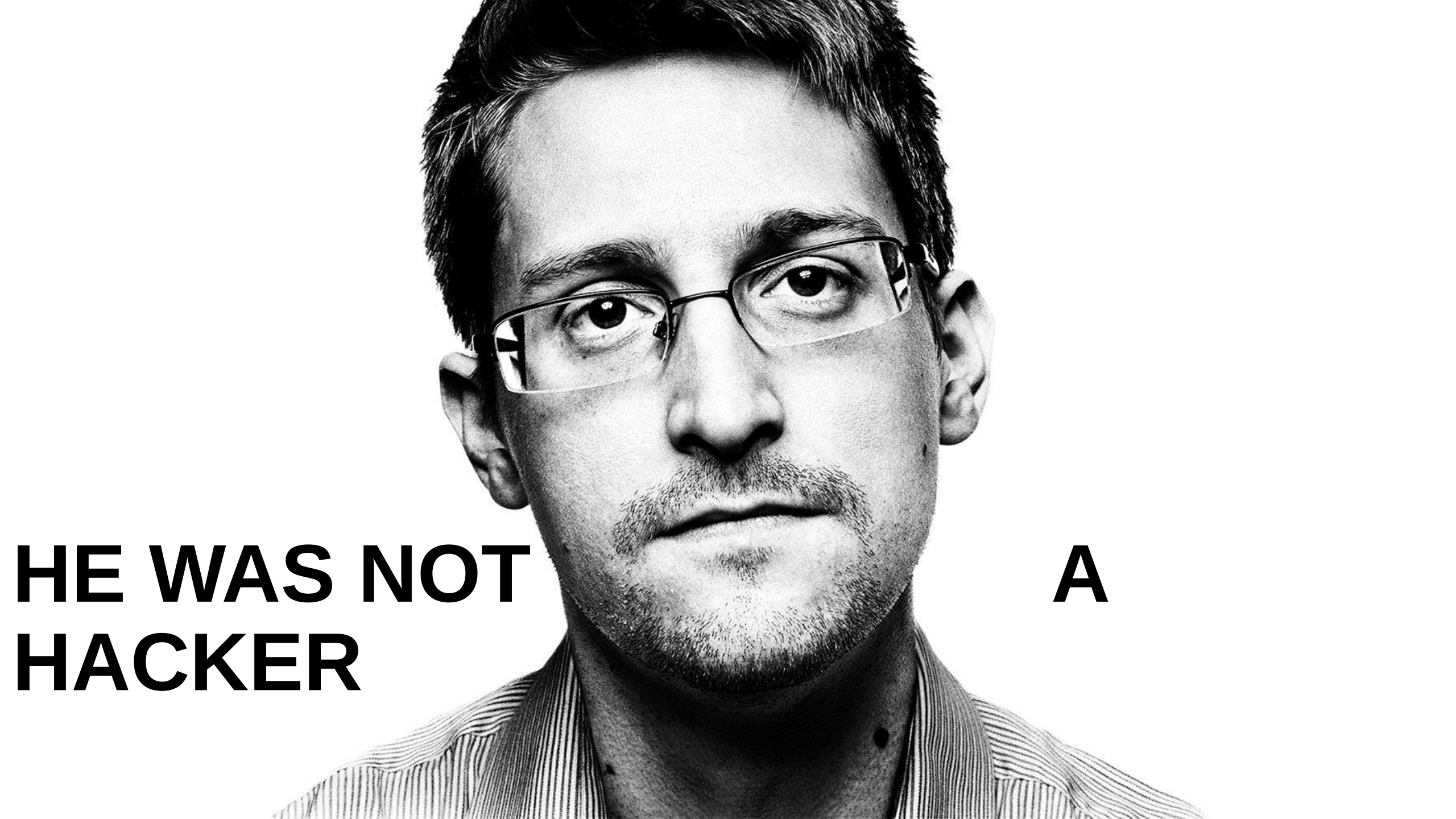


Meet compliance requirements in just few clicks!

Integration with data classification systems

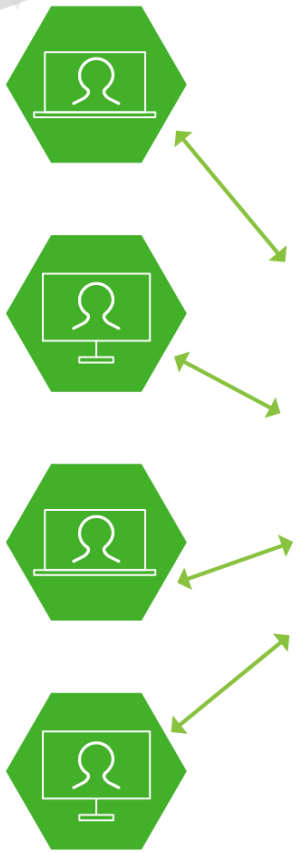
In addition, we can use classification of documents and e-mails sent by users - leveraging data classification systems such as **Microsoft**, **Boldon James**, **Titus**.



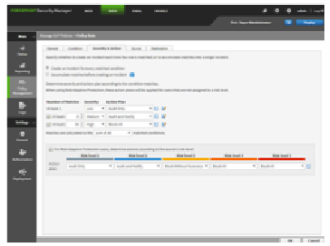

HE WAS NOT A
HACKER

Introducing Dynamic Data Protection

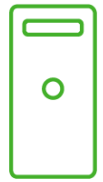
FORCEPOINT DLP



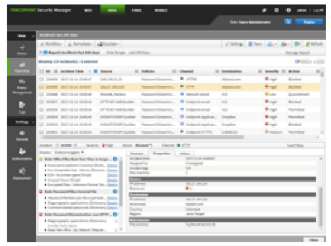
Endpoint Monitoring, Collection & Enforcement



Set dynamic enforcement action plan



Endpoint Server



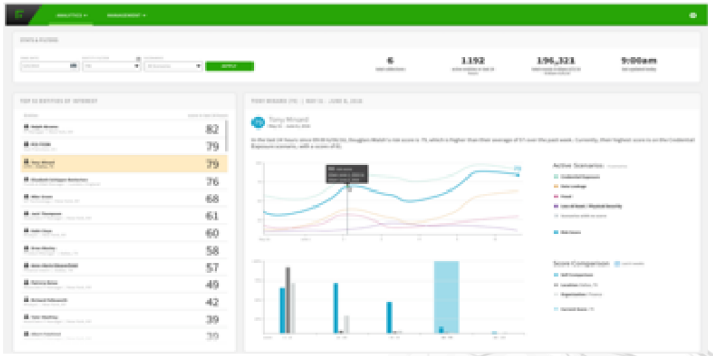
View DLP incidents with end-user risk level

SHARED DATA EXCHANGE

DLP endpoint events and incidents

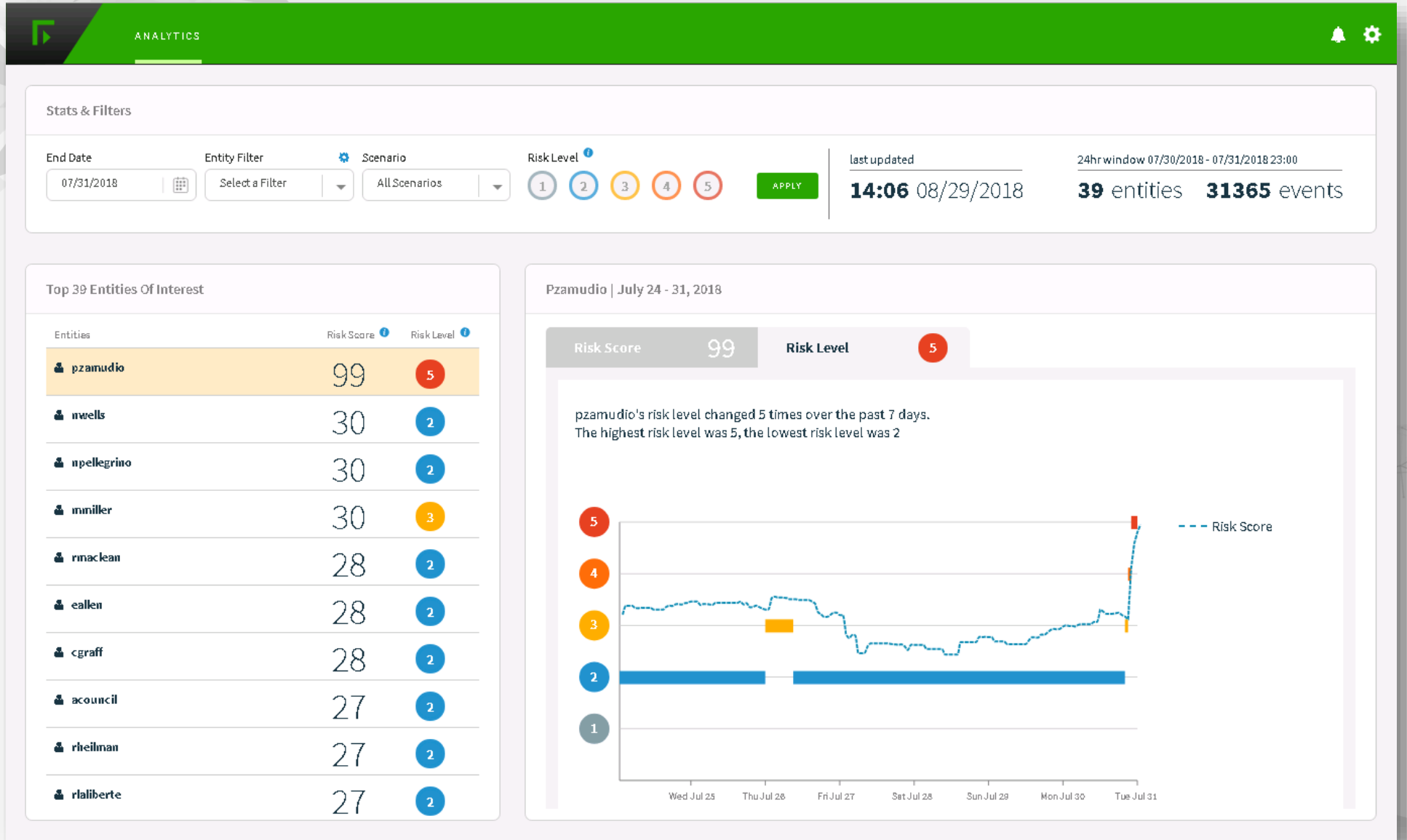
Analytics-calculated entity risk score / levels

FORCEPOINT BEHAVIOR-CENTRIC ANALYTICS



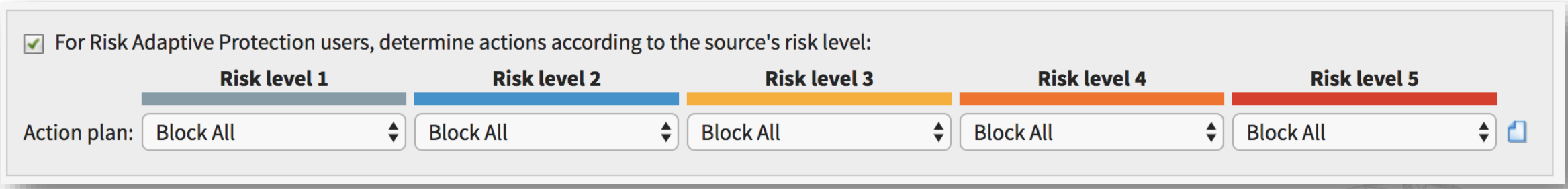
Automatically analyze DLP data for identity risk calculation

Investigate high-risk entity activity

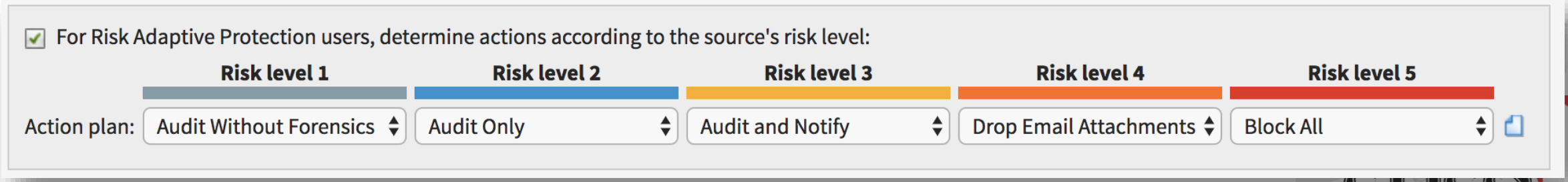


Risk based policy enforcement

For policies governing **compliance use-cases** or **highly sensitive information**,
"Block All" can be the action plan for all risk levels.

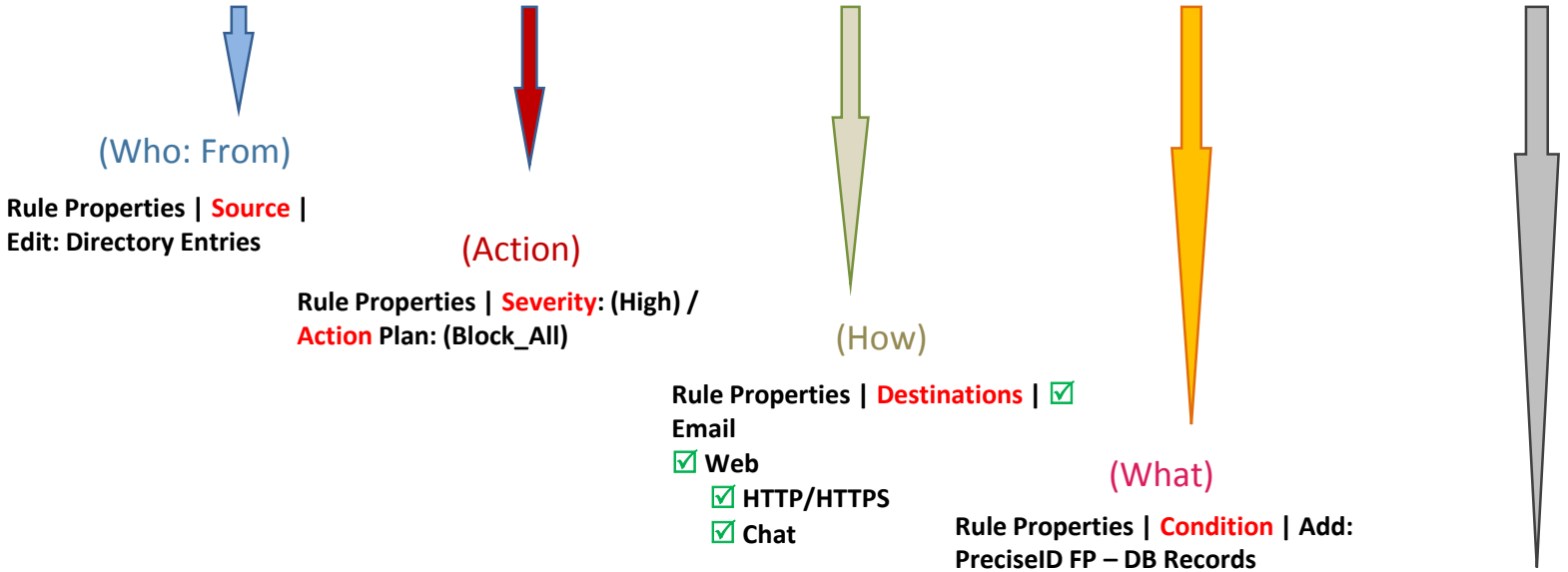


For policies where **additional context** can help **inform decisions**,
Dynamic Data Protection provides additional **granularity**.



Sample data protection policy

Employees **cannot** **send** **customer data** **to…**



(Who: From)

Rule Properties | Source | Edit: Directory Entries

(Action)

Rule Properties | Severity: (High) / Action Plan: (Block_All)

(How)

Rule Properties | Destinations | ☑ Email
☑ Web
☑ HTTP/HTTPS
☑ Chat

(What)

Rule Properties | Condition | Add: PreciseID FP – DB Records

(Who: To)

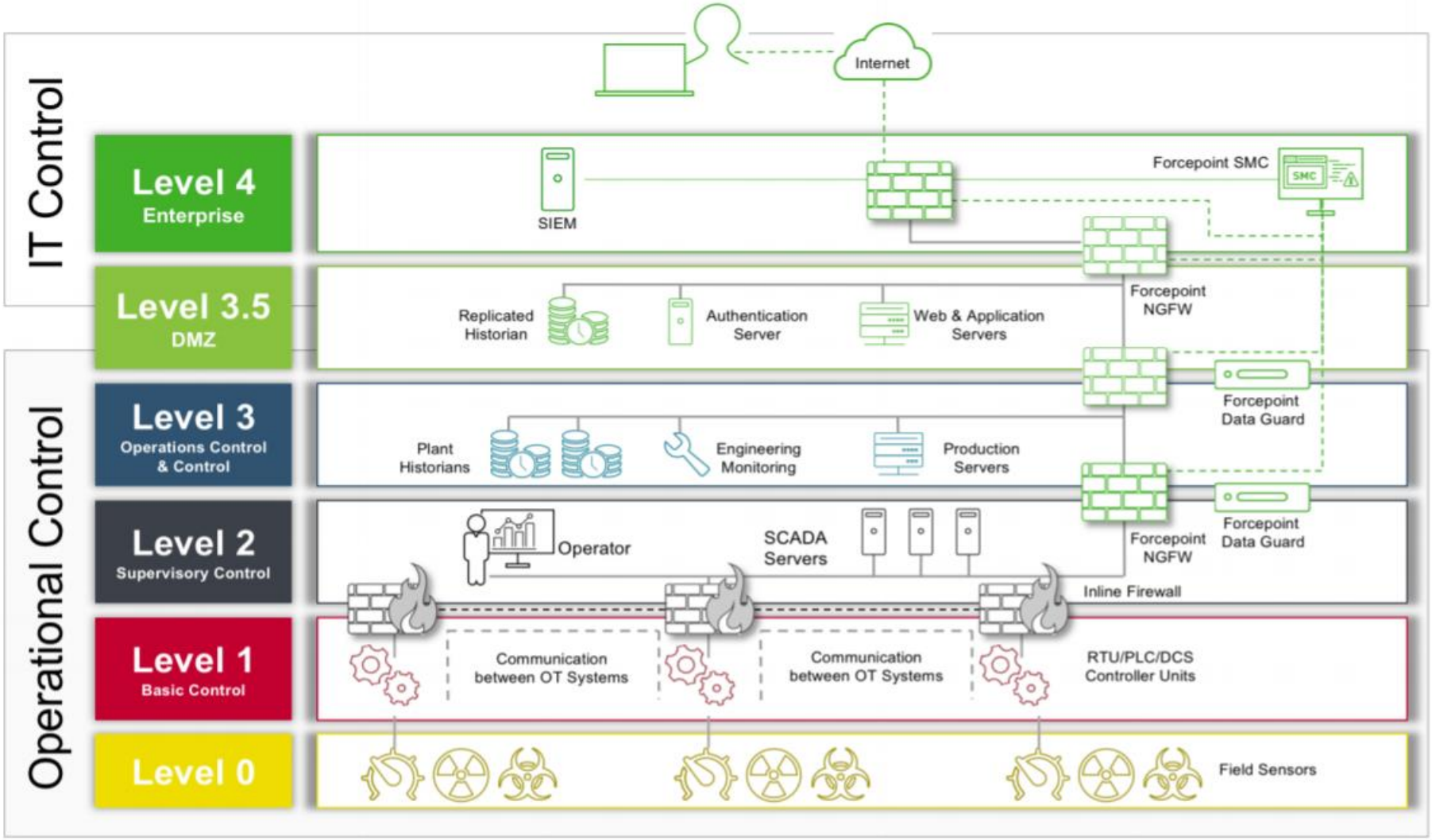
Rule Properties | Destinations | ☑ Email: All
☑ Web: All

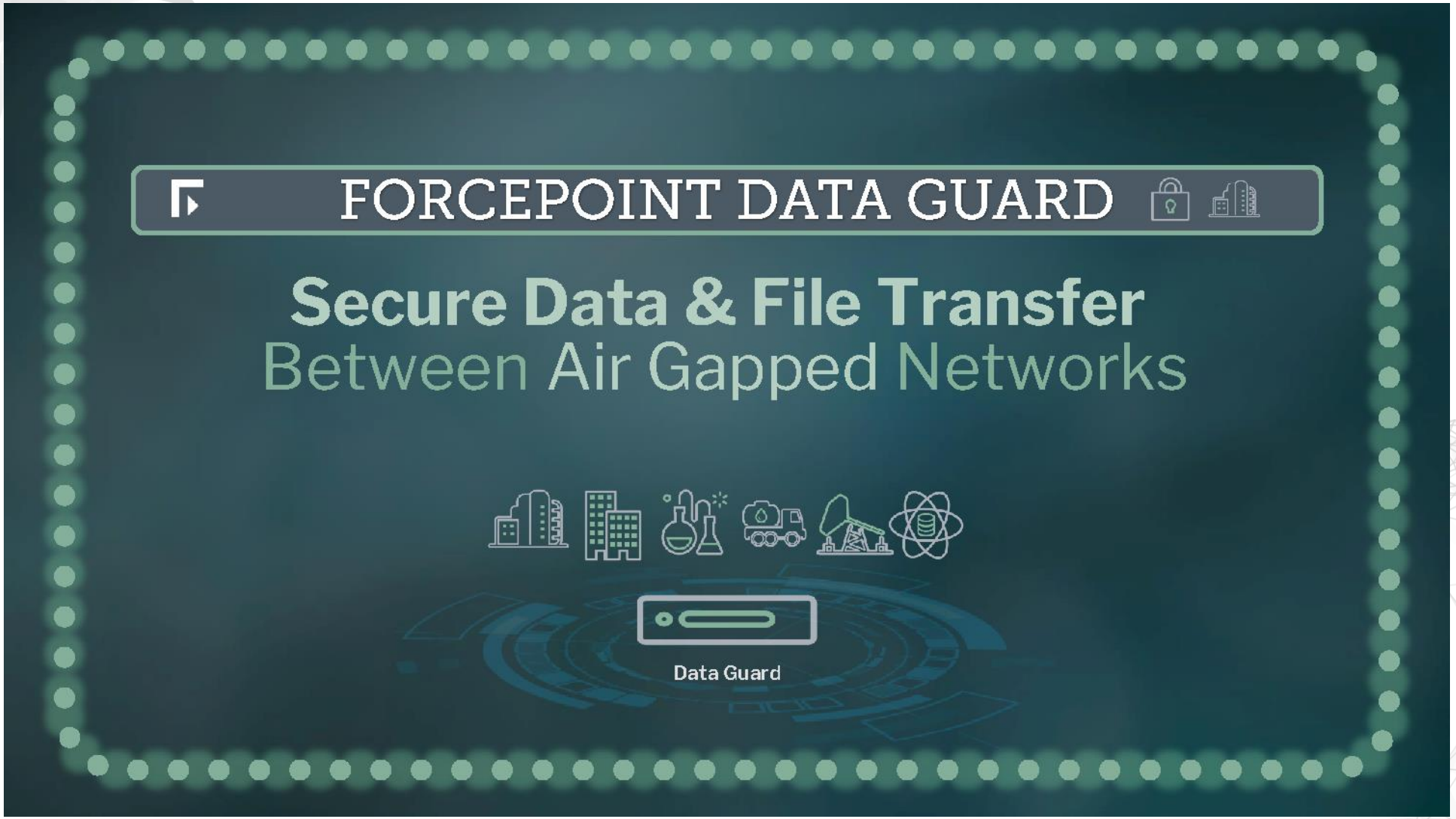
Intelligent process management

Uniform policies cover all aspects of information protection

1. SCADA, ICS, OT – terminology and meaning
2. “Myths” about SCADA security
3. Case study of serious SCADA security incident
4. Attack methods dangerous for SCADA/OT
5. Fundamental principles of SCADA/OT security
6. Good practices in SCADA/OT security projects
7. Vulnerability management and validation in SCADA/OT
8. Dynamic Data Protection(DDP)
9. **Controlling OT and IT connection of SCADA systems**

Conceptual placement of Forcepoint solutions in “always on” environments





FORCEPOINT DATA GUARD

Scenario 1: Secure, Automated File Sanitization and Transfer

Scenario 2: Streamlining SIEM Monitoring (commercial)

Scenario 3: Enabling System Patching/Updates

Scenario 4: Streamlining SIEM Monitoring (critical infrastructure)

FORCEPOINT DATA GUARD

Scenario **1**

CUSTOMER PROFILE

Financial Institution

Financial Institution: Forcepoint DLP customer

- Current business process uses sample data (CSV files and reports) from their production environment (considered a high-security network due to sensitive customer and account data) in their separate, air gapped Test environment.
- Using Forcepoint DLP they check data for Personally Identifiable Information (PII) as users burn data to DVDs to manually move it to the Test environment.
- When PII is detected, users must manually scrub the files and execute the process again.

What keywords do you see?

FORCEPOINT DATA GUARD

Scenario **1**

KEYWORDS

Financial Institution

- **Financial Institution** – potentially highly regulated
- **Current DLP customer** – data security is already a priority
- **Production and Test environments** – potentially 2 separate networks
- **Separate, air gapped** – confirming physical network separation
- **Manually moving data or files** – automation will save them time, money and reallocation of personnel
- **Manually scrubbing data or files** – data or file filtering and sanitization is automated in the Guard; more reliable, faster, auditable

How can you HELP this customer automate processes and extend their data security?

FORCEPOINT DATA GUARD

Scenario **1**

HOW TO HELP THE CUSTOMER

Financial Institution

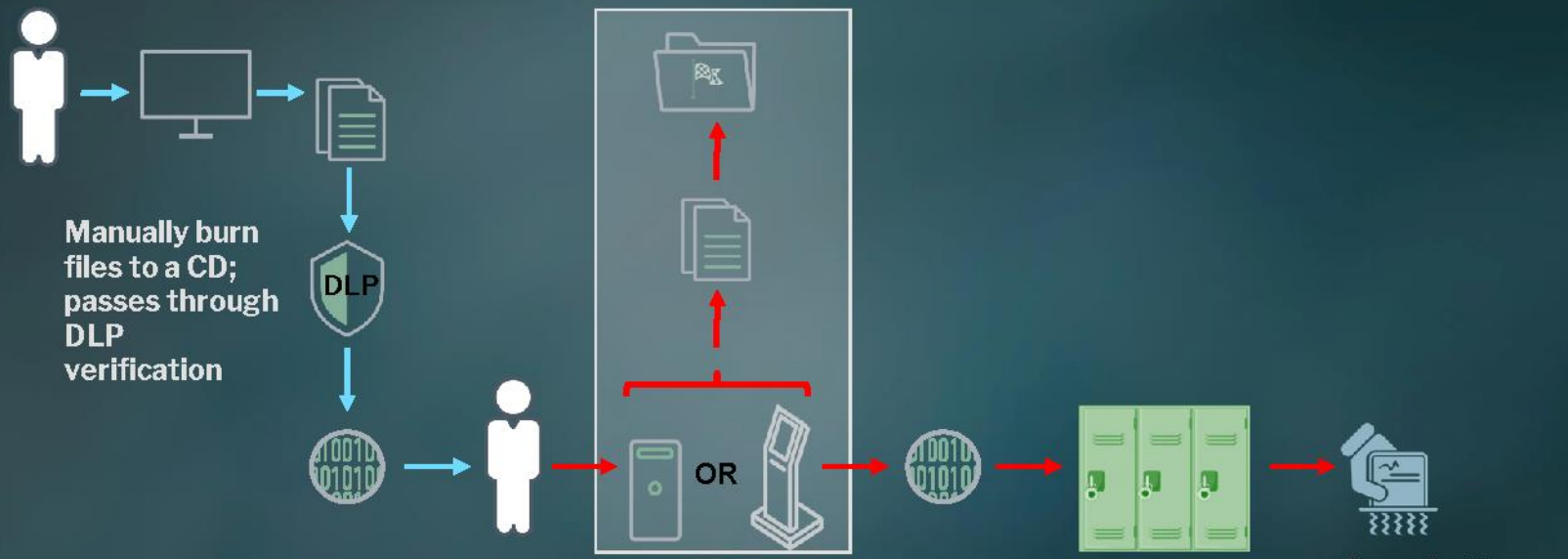
UPSELL – **DATA GUARD**: Extending Existing DLP Protections with Secure, Automated File Sanitization and Transfer.

Benefits:

- DLP validates file does not contain PII
- DLP places "cleared" files in a watch directory
- Data Guard picks up the files (through file drop plugin) and does a second round of filtering – sanitizing files as needed
- Files that pass / pass with sanitization are then AUTOMATICALLY moved to the separate TEST network
- NO manual processes needed, no DVDs needed, no more sneakernet. Just click and drag!

Let's See How it works: ⇨

Scenario 1 (Before): File Transfer without Data Guard



Manually burn files to a CD; passes through DLP verification

Manually copy files from CD to destination via separate network terminal or kiosk.

Requires:

- Antivirus separate license
- Data Sanitization separate license
- Kiosk solution separate product

User securely stores the CD

Organization ensures secure CD destruction

Scenario 1 (After): File Transfer with Data Guard

NETWORK A
User copies files to a designated local folder on Network A. DLP validates copy action is allowed.

NETWORK B
Data Guard monitors folder, grabs files, performs inspections then moves files to specified destination folder.

- Antivirus
- File Typing
- Data Sanitization
- Watermark (PDFs)

With the Guard: One step for secure file movement between air gapped networks

- Guaranteed inspection
- Full end-to-end audit trail
- One vendor for support

FORCEPOINT DATA GUARD

Scenario **2**

CUSTOMER PROFILE

Global Conglomerate SOC

Global Conglomerate has a single regional Security Operations Center (SOC) that is responsible for: (amongst other things)

- Security incident and event monitoring (SIEM) of users and networks from 3 separate business units.
- Currently, administrators and analysts must monitor separate SIEM dashboards – 1 (or more) for each business unit.
- Manually piece together log and reporting data for daily and weekly "security state" reports for Corporate.

What keywords do you see?

FORCEPOINT DATA GUARD

Scenario **2**

Global Conglomerate SOC

KEYWORDS

- **3 separate business units** – confirming physical network separation
- **Separate SIEM dashboards** – automation is more accurate, will save them time, money and reallocation of personnel
- **Manually creating reports** – combining the SIEM data to 1 location through the Guard allows for a holistic view and more accurate, automated reporting

How can you HELP this customer gain a holistic view of their enterprise security and reduce burden and errors?

FORCEPOINT DATA GUARD

Scenario **2**

HOW TO HELP THE CUSTOMER

Global Conglomerate SOC

NEW OPPORTUNITY – **DATA GUARD + NGFW**:
Streamlining SIEM Monitoring in a Multi-Network Environment

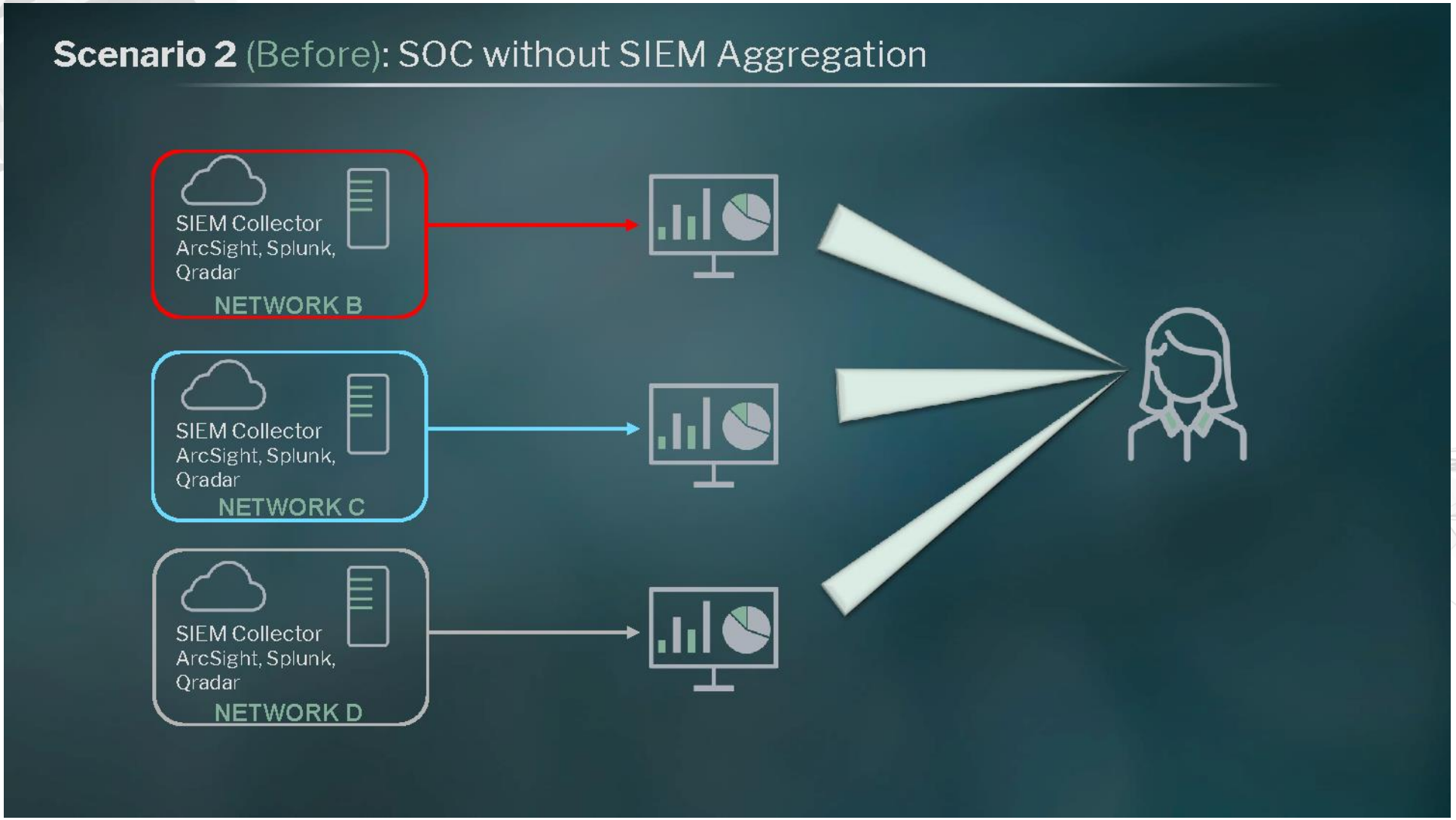
Benefits - **Data Guard**:

- Automated, streamlined data aggregation
- Holistic view of the enterprise from a single pane of glass
- Correlation of events across networks – seeing similar anomalous behavior on multiple networks can provide clues or indicate breadth of breach
- Personnel reassignment to other critical tasks
- Flexibility to support almost any standard or custom messaging protocol, while still providing extensive security controls on all transmissions.

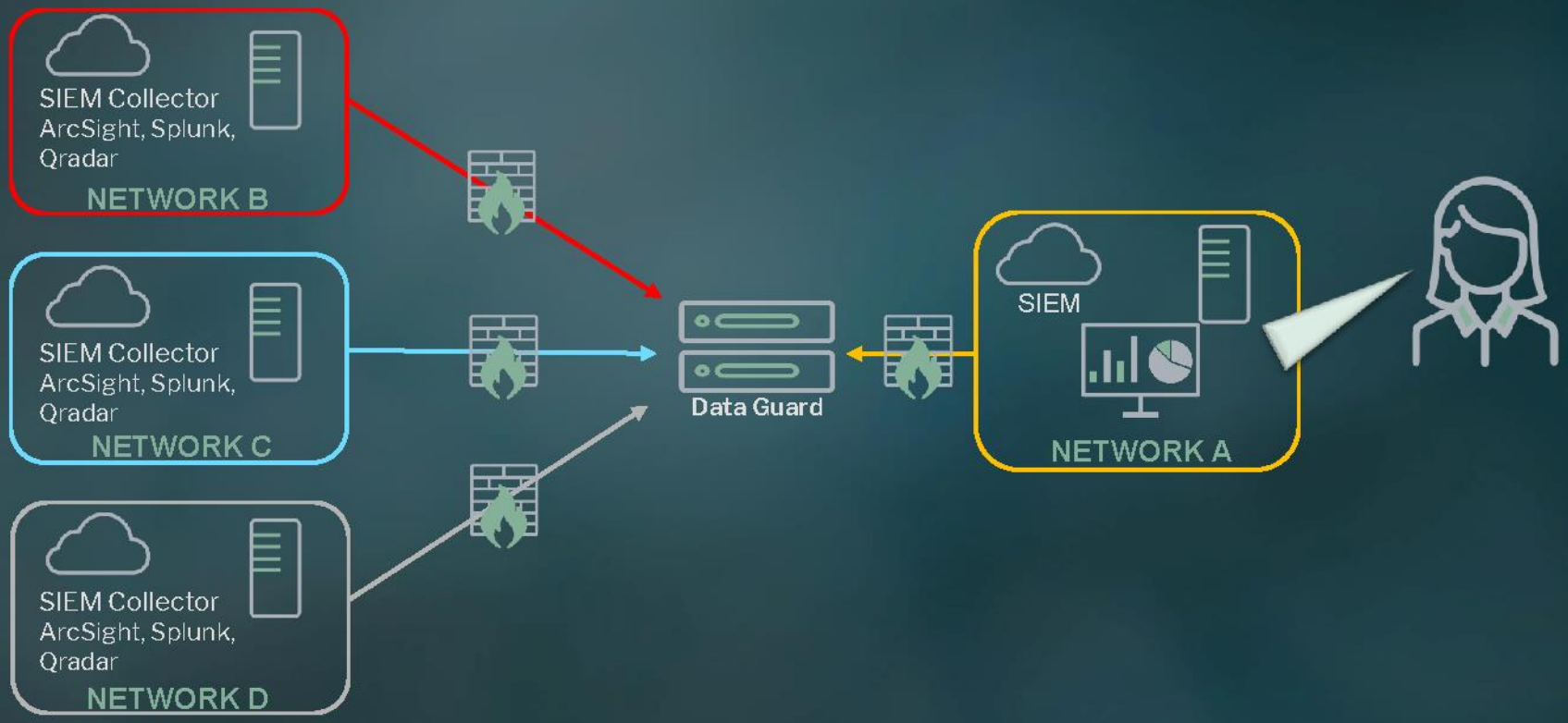
Benefits – **NGFW**:

- High Availability - utilize NGFW load balancing capabilities with central management and reporting
- Additional Protection - filter protocols, source/destination, etc. at the firewall first. Provides defense in depth and cyber security protections such as Denial of Service protections.

Let's See How it works: ⇨



Scenario 2 (After): 1 Guard Pair Connected to Multiple Networks
SOC with SIEM Aggregation



FORCEPOINT DATA GUARD

Scenario **3**

CUSTOMER PROFILE

Ministry of Defence

Ministry of Defence customer

- Utilizes 3 physically separated, air gapped and closed networks that reside in different buildings.
- They endeavor to be very diligent about patching all applications and network devices but – well, sometimes there are more pressing matters to attend to
- Can take a while to get all the necessary approvals and physically get to each location. Another rising challenge is a CIO mandate to ban USBs on all Defence systems. **Without a USB, how will the administrator get the patches on to the closed systems?**

What keywords do you see?

FORCEPOINT DATA GUARD

Scenario **3**

Ministry of Defence

KEYWORDS

- **Ministry of Defence** – government customer, highly sensitive environments and data
- **Separate, air gapped** – confirming physical network separation
- **Manually moving data or files** – automation will save them time, money and reallocation of personnel
- **Ban on USBs** – change in policy for which the customer must prepare

How can you HELP this customer automate processes and extend their data security?

FORCEPOINT DATA GUARD

Scenario **3**

HOW TO HELP THE CUSTOMER

Ministry of Defence

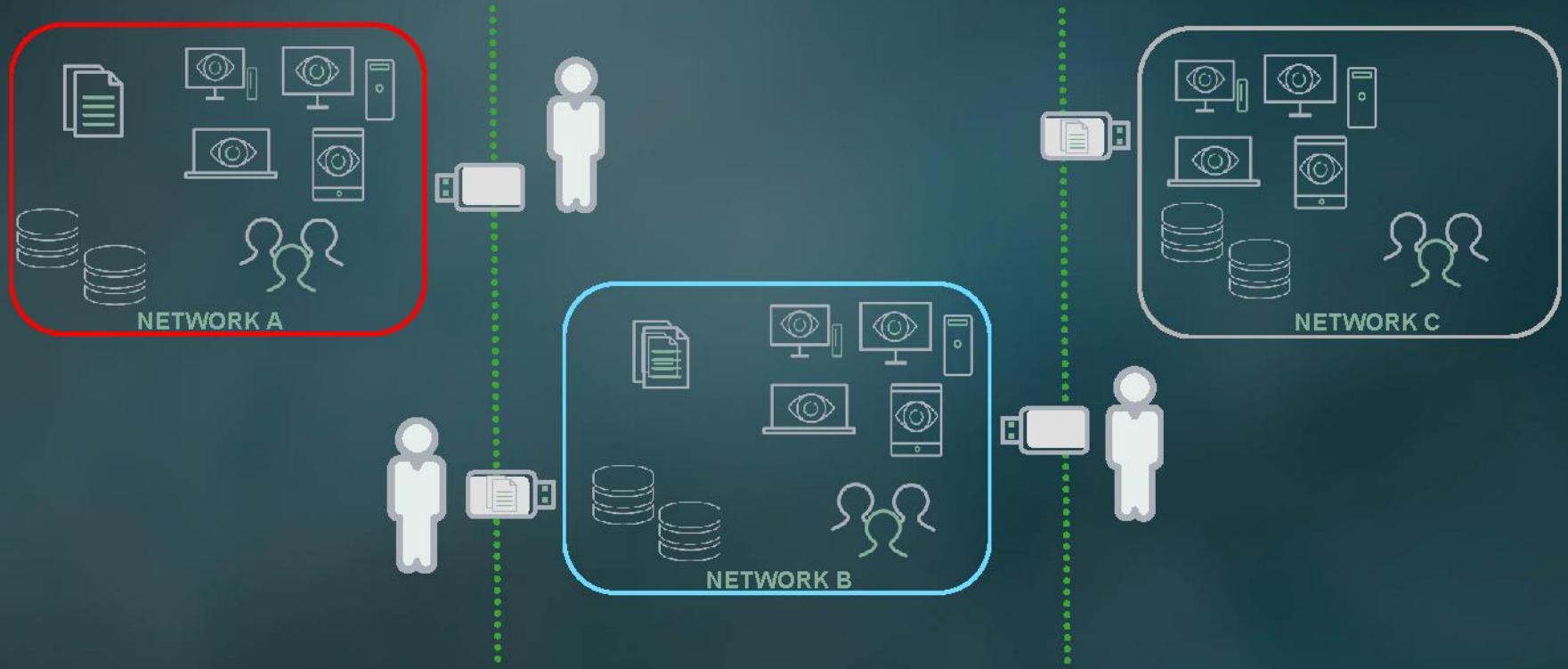
NEW OPPORTUNITY – **DATA GUARD**:
Enabling System Patching/Updates in a Closed Environment

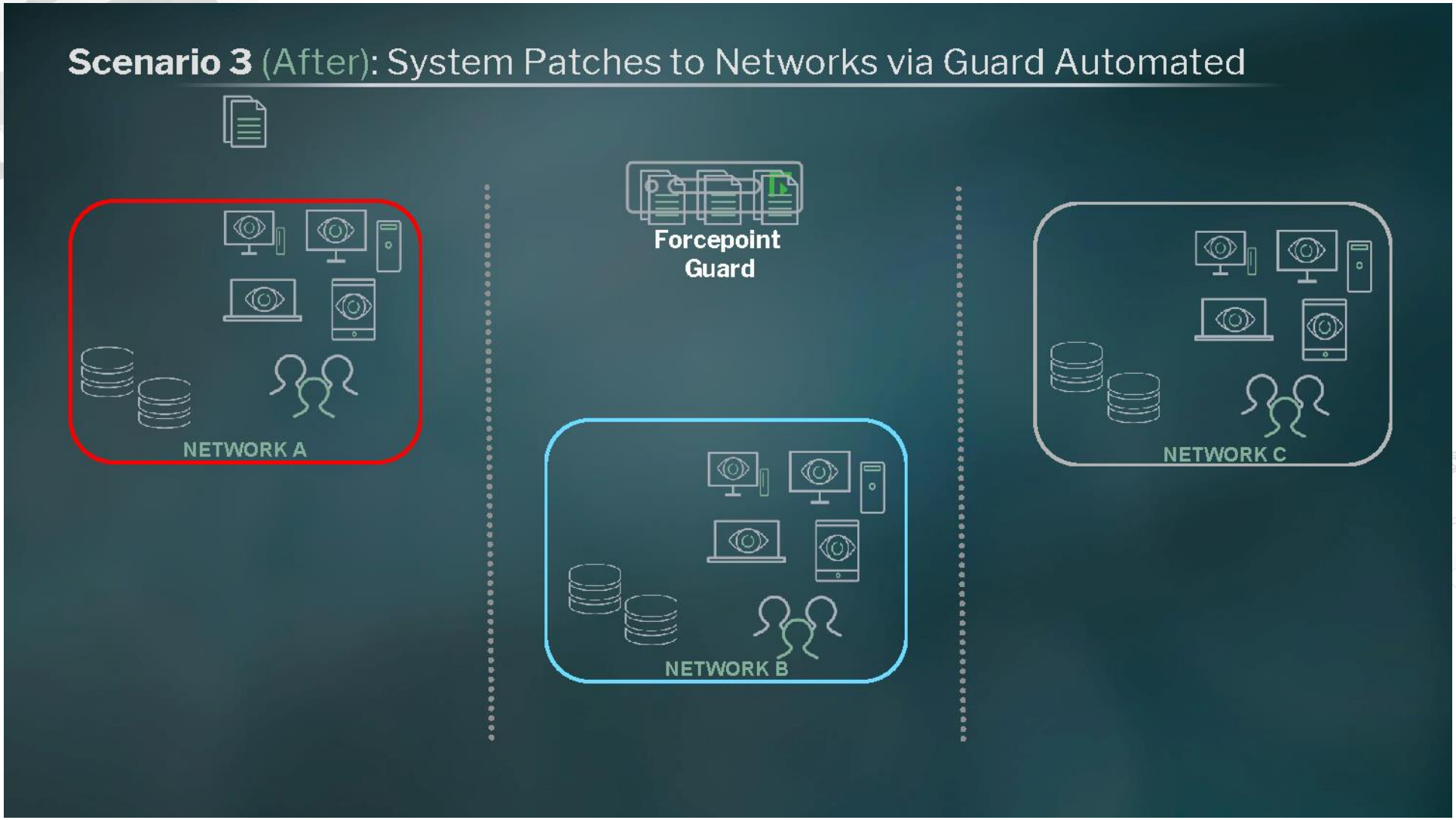
Benefits:

- The admin sends files to the Guard – or uses an automated process
- The Guard validates and verifies the files against its transfer policy rules for all destination networks
- Files pass all checks, the Guard transfers them to all destination networks – ready to be applied
- NO manual processes needed, no USBs needed, no more sneakernet

Let's See How it works: ⇨

Scenario 3 (Before): System Patches to Networks Manually





FORCEPOINT DATA GUARD

Scenario **4**

CUSTOMER PROFILE

Manufacturing Plant SOC

Manufacturing Plant has a Security Operations Center (SOC) responsible for: (amongst other things)

- Security incident and event monitoring (SIEM) of users and networks. Currently, the administrators are only able to monitor endpoints located on the IT network.
- They are undergoing an IT-OT convergence that is placing the full cybersecurity responsibilities with the CISO.
- CISO wants a secure way to streamline all the SIEM traffic into the current SOC infrastructure rather than having to pay for all the extra gear and licenses.
- Currently administrators and analysts must monitor separate SIEM dashboards – 1 (or more) for each operational system – and manually piece together log and reporting data for daily and weekly "security state" reports for leadership.

What keywords do you see?

FORCEPOINT DATA GUARD

Scenario **4**

Manufacturing Plant SOC

KEYWORDS

- **IT-OT convergence** – confirming physical network separation AND need to connect “the unconnectable”
- **Separate SIEM dashboards** – automation is more accurate, will save them time, money and provide a more holistic view of the full IT-OT enterprise
- **Manually creating reports** – combining the SIEM data to 1 location through the Guard allows for a holistic view and more accurate, automated reporting

How can you HELP this customer gain a holistic view of their enterprise security and reduce burden and errors?

FORCEPOINT DATA GUARD

Scenario **4**

HOW TO HELP THE CUSTOMER

Manufacturing Plant SOC

NEW OPPORTUNITY – **DATA GUARD + NGFW**:
Streamlining SIEM Monitoring in a Plant Environment between IT and OT

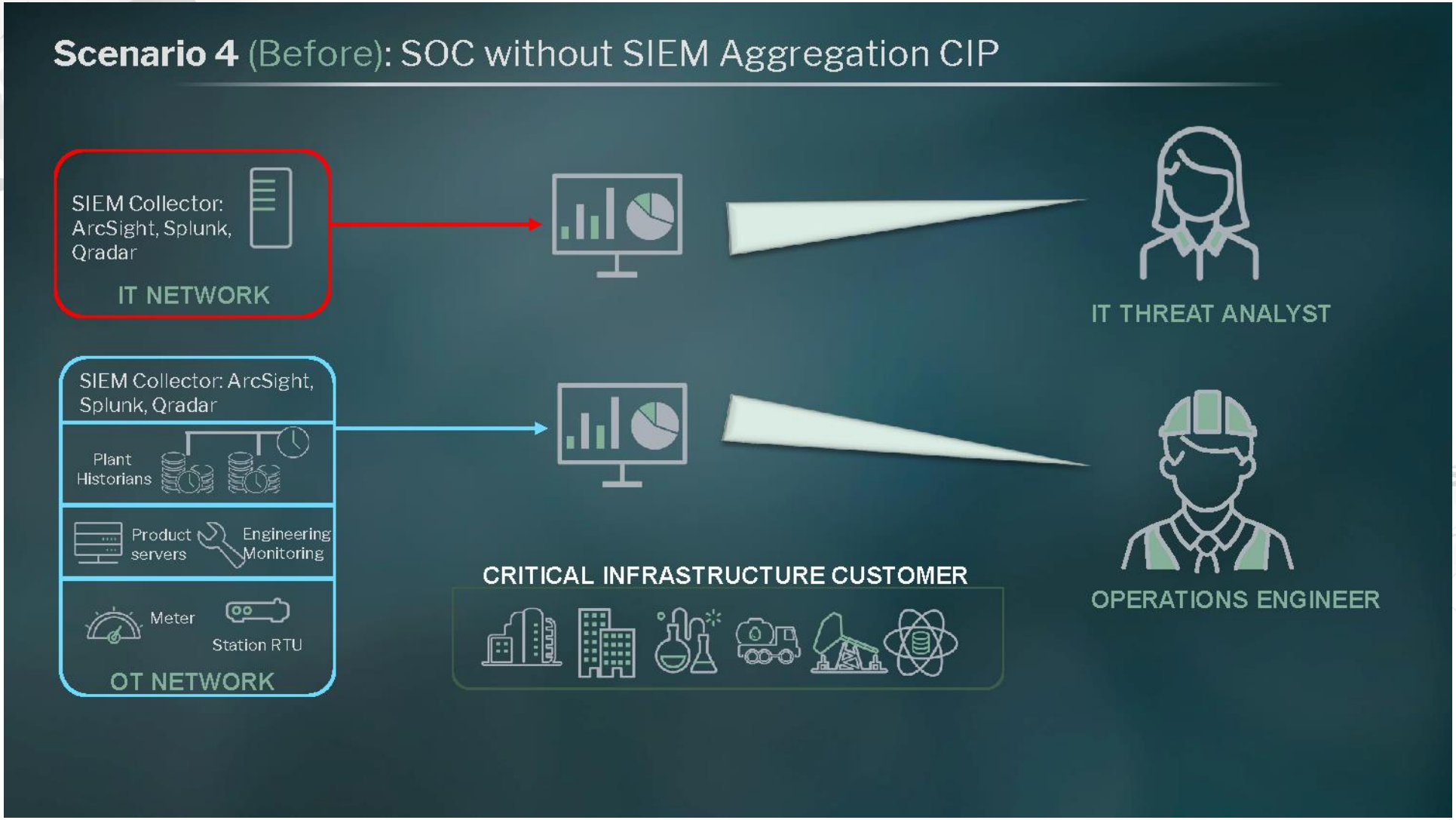
Benefits - **Data Guard**:

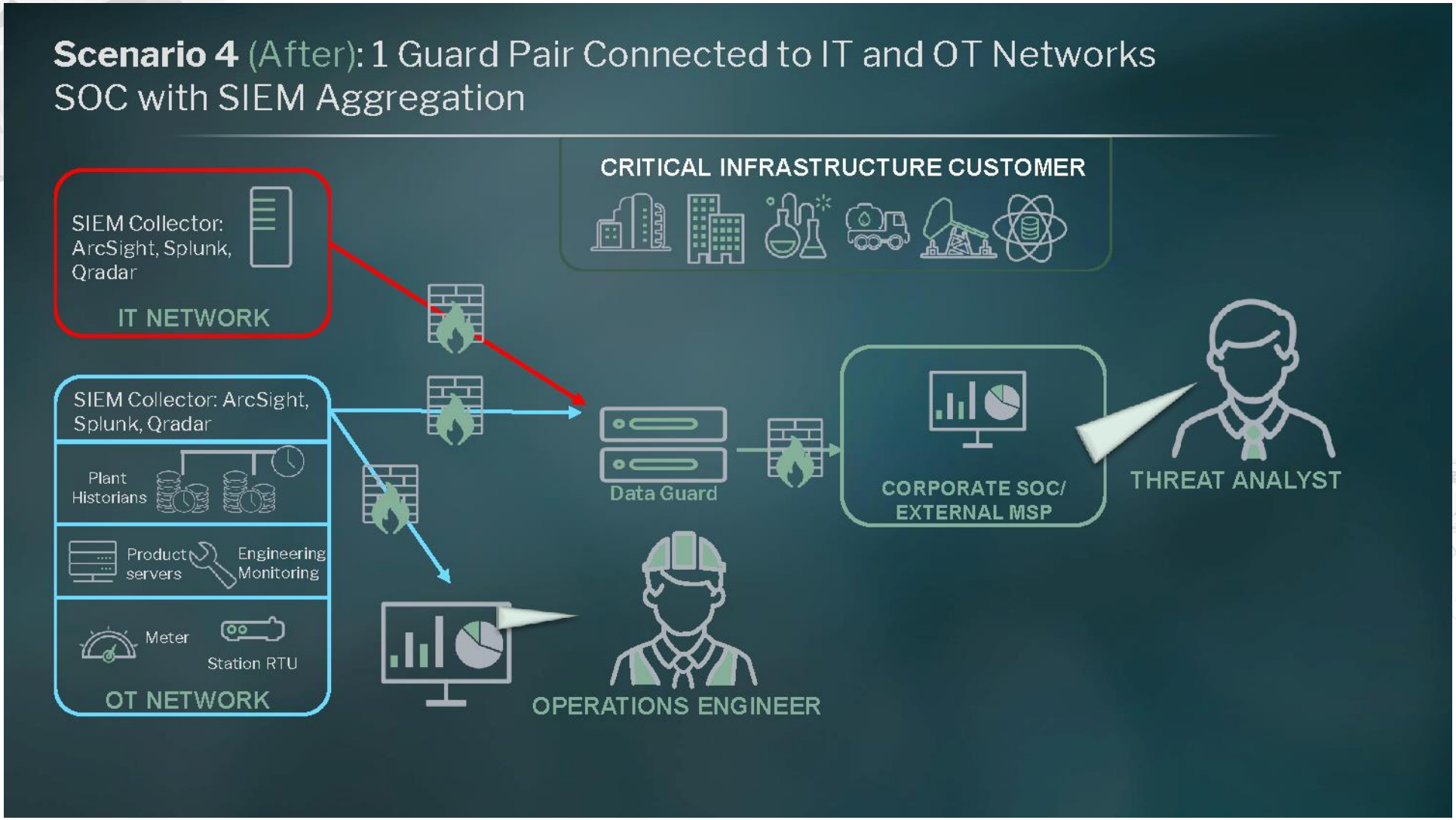
- Automated, streamlined data aggregation
- Enables holistic view of the enterprise from a single pane of glass
- Correlation of events across networks – seeing similar anomalous behavior on multiple networks can provide clues or indicate breadth of breach
- Allows for more efficient use of SIEM technology and SOC staff
- Flexibility to support almost any standard or custom messaging protocol, while still providing extensive security controls on all transmissions.

Benefits – **NGFW**:

- Defense-grade firewalls deliver higher resilience, threat efficacy, and unified management capabilities
- Security that fits the unique nature physically separated assets, mixed-vintage assets, and decentralized facilities management.

Let's See How it works: ⇨





Kako dobiti dodatne informacije?

sales@clico.rs

support@clico.rs

Vaš distributer sa dodatnom vrednošću!

HVALA!