BLUEPRINT FOR SECURING INDUSTRIAL CONTROL SYSTEMS

PREFACE

At about midnight on Monday March 18, 2019, one of the world's largest aluminum producers, with smelting plants, factories and offices in 40 countries, noticed irregularities in its systems. Hours later, Norway-based Norsk Hydro confirmed it was suffering production stoppages in Europe and the US as it battled a major ransomware attack, forcing the company to switch to manual operations while it attempted to contain the issue.

Ransom was never paid, but the total cost of the attack was estimated to be around $52 million.

A few days later, 2 other US-based chemical companies, Hexion and Momentive, were also hit by cyber attacks and had to shut down IT systems to contain the incidents. The same encryption program called LockerGoga is thought to be behind all three attacks.

The attack had a tremendous impact on the production of aluminum worldwide. [1]

This whitepaper is written as a guide to securing networks with Critical Infrastructure in order to prevent similar catastrophes from happening again.

OVERVIEW

In order to secure Critical Infrastructure environments, it is vital to keep a holistic view and look at every part of the network, both the IT (Information Technology) and OT (Operational Technology) parts, investigate the systems and processes in each zone, analyze the attack vectors and risk, and provide recommended security controls.

In order to do so, we use the Purdue model, which was adopted from the Purdue Enterprise Reference Architecture (PERA) model by ISA-99 and used as a concept model for Computer Integrated Manufacturing (CIM). [3] It is an industry adopted reference model that shows the interconnections and interdependencies of all of the main components of a typical Industrial Control System, dividing the ICS architecture into 3 zones and subdividing these zones into 6 levels.

THE PURDUE MODEL

The two major zones are the Enterprise and Manufacturing Zones, also referred to as the IT and OT networks. In the Purdue model, these two major zones are separated by the third zone, the Industrial DMZ, where the intent is to prevent direct communication between IT and OT systems. This adds a layer of separation to the overall architecture so that if something were to compromise a system in the DMZ, then the compromise could be contained within the DMZ, ensuring production processes continue to operate normally.

IT Zone

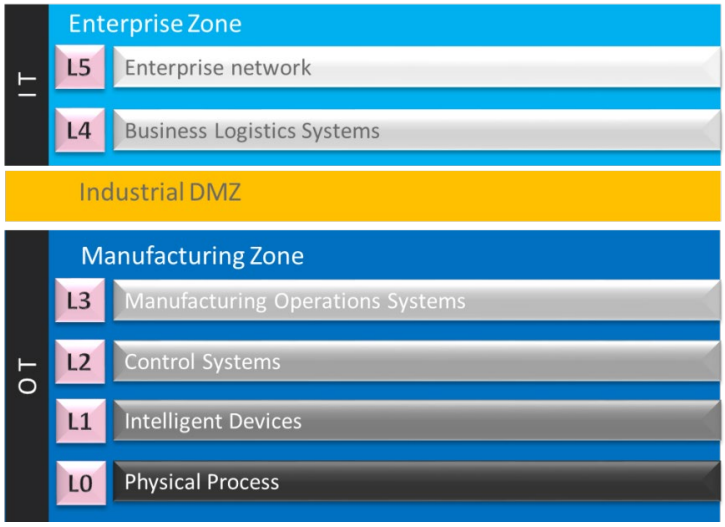
Level 5: Enterprise Network
Technically not part of ICS, the enterprise zone relies on connectivity with the ICS networks to feed the data that drives the business decisions.

Level 4: Business Logistics Systems
Enterprise Resource Planning (ERP) systems manage the business-related activities of the manufacturing operation. It establishes the basic plant production schedule, material use, shipping and inventory levels.

Industrial DMZ:
The interconnect zone between IT and OT systems, this zone typically holds a jump host for secure remote access to ICS systems.

OT Manufacturing Zone

Level 3: Manufacturing Operations Systems
The purpose of level 3 systems is to manage production workflows to produce the desired products. This includes: batch management; manufacturing execution/operations management systems (MES/MOMS); laboratory, engineering stations, maintenance and plant performance management systems; data historians and related middleware.



Level 2: Control Systems
Level 2 systems supervise, monitor and control the physical processes. This includes real-time controls and software; Distributed Control System (DCS), human machine interface (HMI); supervisory and data acquisition (SCADA) software.

Level 1: Intelligent Devices
Level 1 systems sense and manipulate the physical processes. This includes process sensors, analyzers, actuators and related instrumentation such as PLCs, RTUs or IEDs.

Level 0: Physical Process
Level 0 systems define the actual physical processes.

APPLYING SECURITY TO ICS

In this document, we will dissect the 6 different layers explained above and how they map to different areas in the network. The purpose is to explain the communication flows between the different levels in the Purdue model and how Check Point recommends they should be secured. In order to do so, the following diagram will be used as an example.

The diagram is a high-level representation of a typical IT/OT environment. However, the link between level 2 and 3 may vary depending on the organization type.

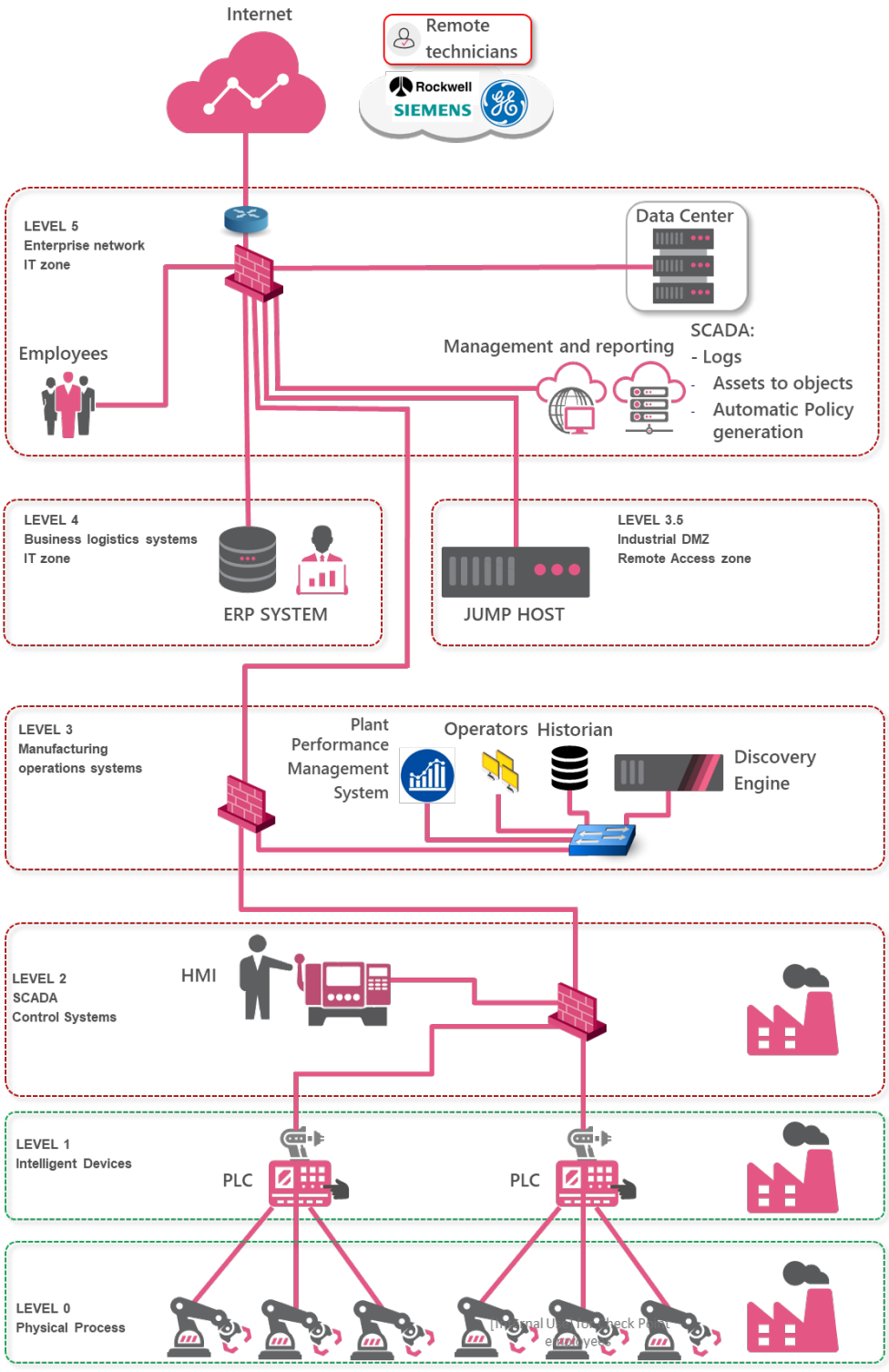
- Manufacturing plants are typically a single-site that combines both OT and IT
- Utilities and energy such as gas, water and electric are typically distributed environments with many remote sites communicating back to a central facility. Bandwidth constraints may affect the proposed architecture.

The Check Point components offered in this whitepaper are:

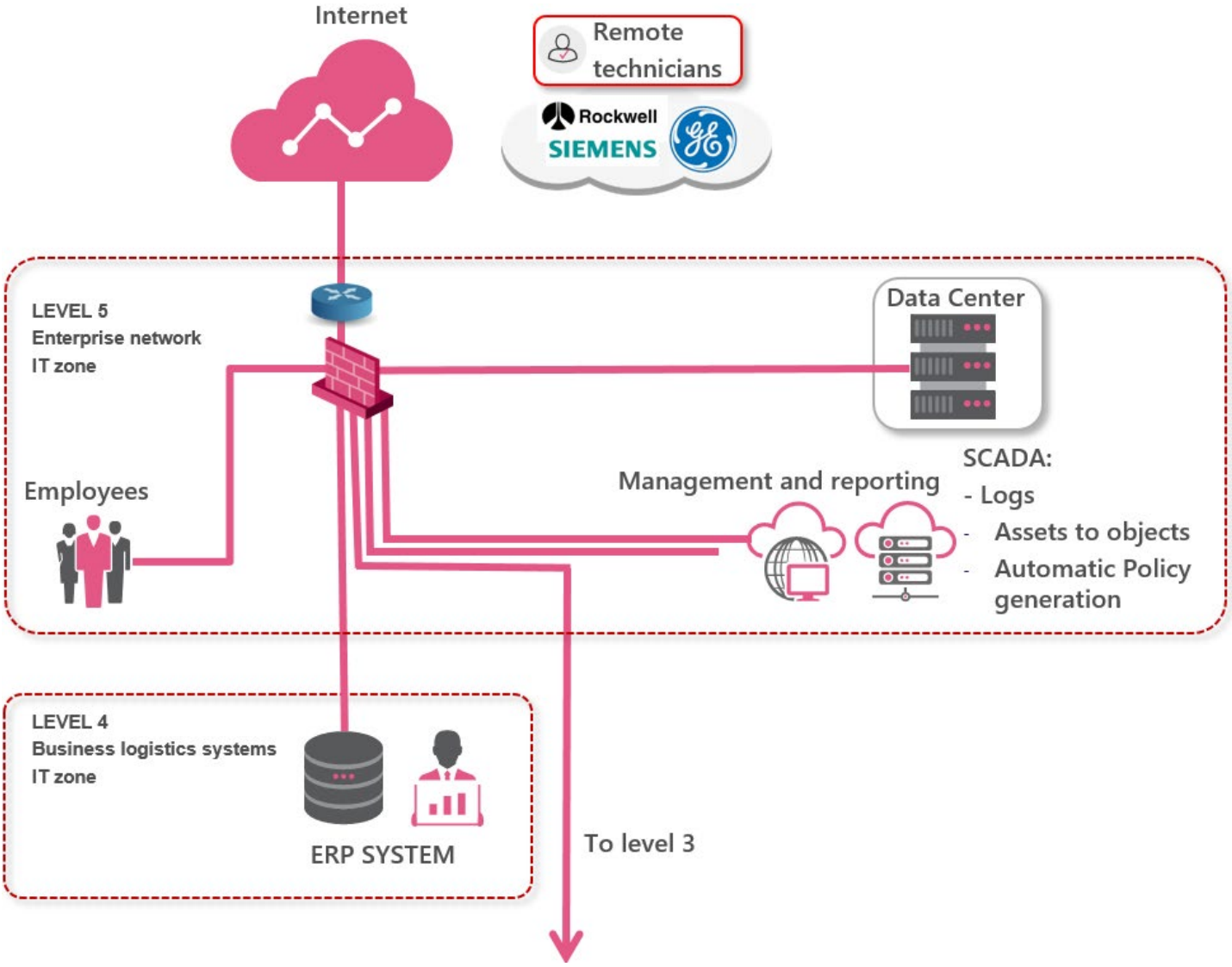
- Check Point Security Gateways (including threat prevention technologies)
- Check Point Endpoint Security
- Check Point Management
- A third party discovery engine

Check Point has strategic partnerships with several 3rd party Discovery Engine vendors. Some focus on specific verticals like Critical Infrastructure, Healthcare, Building Management Systems or IoT, some focus on several verticals at the same time. For a full list of strategic partnerships for ICS, please visit https://www.checkpoint.com/solutions/industrial-control-systems/

In the example in this whitepaper, the 3rd party Discovery Engine used is Claroty. It constantly monitors industrial control system (ICS/SCADA) network traffic and generates alerts for anomalous network behavior that indicates a malicious presence or changes that have the potential to disrupt the industrial processes.



Level 5 and 4: The Enterprise IT Network and Business Logistics Systems



Systems and Processes:
This is the IT part of the network where the users, Data Center and cloud access are located. This is also the part of the organization where the Internet break-out is found.

Attack Vectors:
Typical IT attack vectors, such as spear phishing via Email and Ransomware against users and endpoints.

Industry Example:
In June 2019, an aircraft parts manufacturer called ASCO Industries fell victim to a ransomware attack. According to reports, most of the company's systems, based in Zaventem, Belgium, were affected by the infection, leading to an entire month of inactivity in the IT infrastructure of all ASCO plants. This caused more than a thousand out of the 1,500 employees at ASCO's headquarters in Belgium to be sent back to their homes, since conditions were not optimal to maintain operations.

Risks:
Infrastructure attacks are a relevant and imminent threat to any organization. Many of the recent attacks on OT and ICS networks were found to be based on IT attack vectors.

Recommended Security Controls:

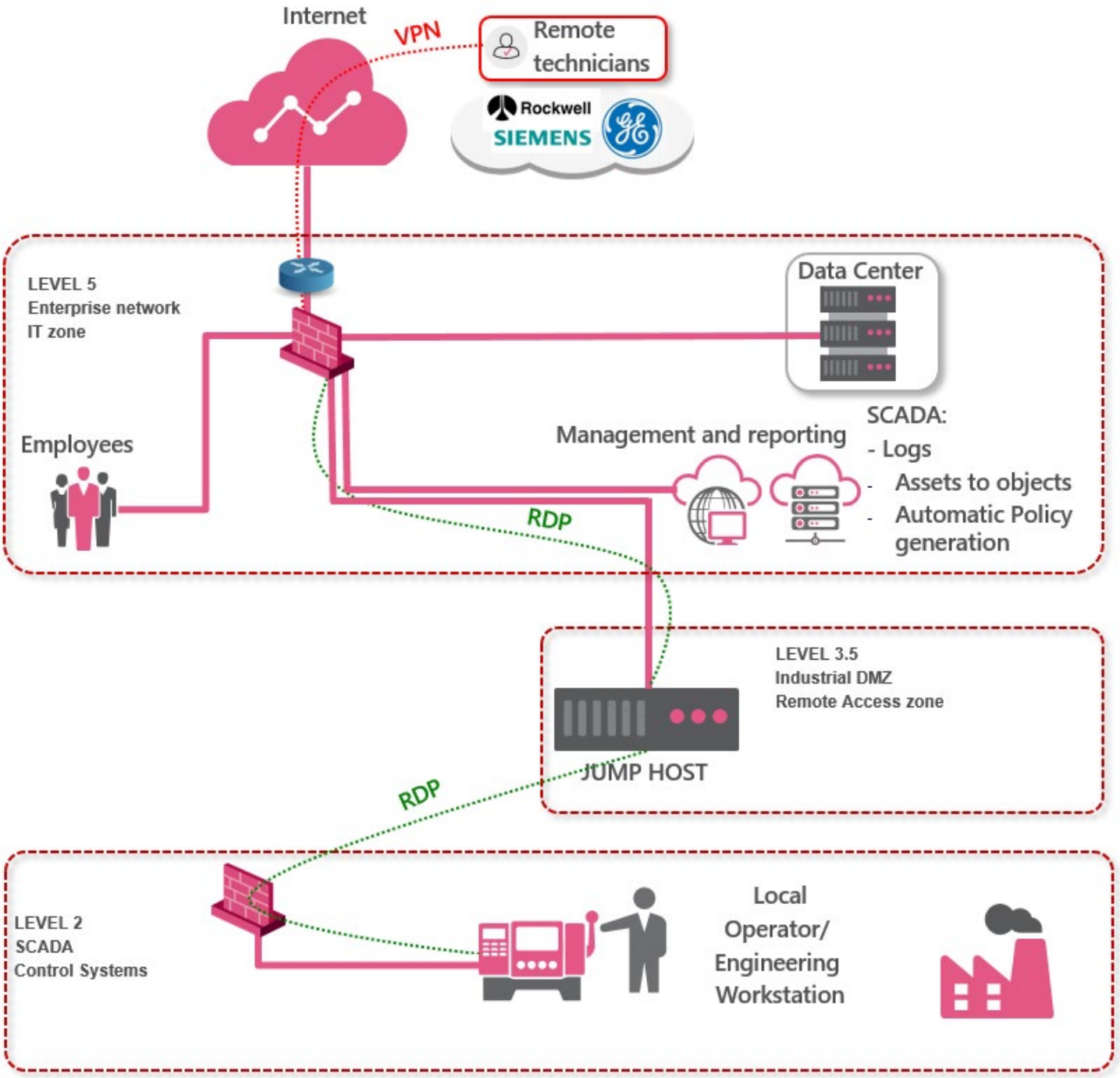
As this is the IT network where the users reside and this is where the internet egress point is located, it is recommended to enable the full Next Generation Threat Prevention plus SandBlast Zero-day Protection (sandboxing) feature set on the network level:

- Firewall
- IPS
- Antivirus
- Anti-bot
- SandBlast (sandboxing)
- Application Control
- URL Filtering
- SSL inspection

It is also recommended to install the full Check Point Endpoint Security suite on the users' machines.
Last but not least, it is very important to secure public cloud services, as these are usually connected to corporate resources and therefore also a potential attack vector.

Enabling network and endpoint security can prevent and eliminate the attacks prior to breaching the ICS equipment. The Security Management server manages all of the security gateways mentioned in this blueprint.

Level 3.5: The Industrial DMZ



Systems and Processes:

Typically, this part of the network is used for technicians' remote access connections. They can work for the company or the inbound connections that originate from the supplier of the equipment used in the OT network.

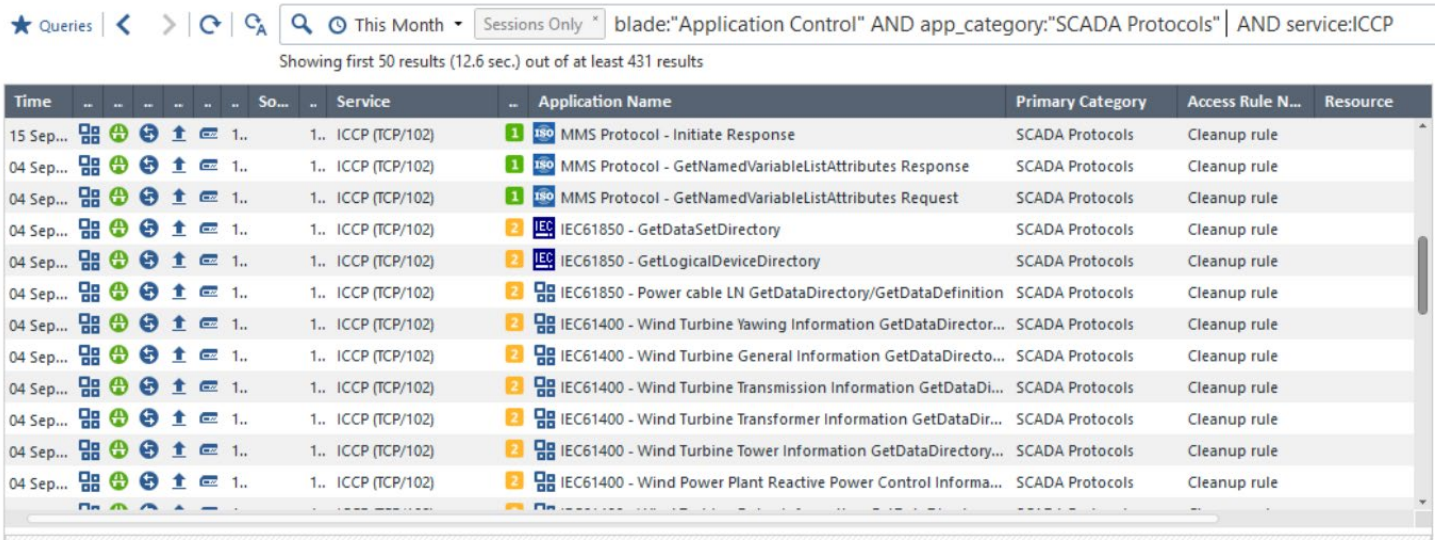
Attack Vectors:

- Systems that are exposed directly without VPN technology can easily be exploited
- Malware entering the organization's OT network over a remote access connection
- Denial of Service attacks on the remote access gateway

Industry Example:
Thousands of critical energy and water systems exposed online for anyone to exploit.

Risks:
In some cases, OT equipment suppliers demand direct IP connectivity to OT equipment in Layer 2 and 1 for support, monitoring and maintenance. This can be a hazardous operation if there are no adequate security controls in place to properly inspect this traffic. If the security standards of a third party connecting straight into the OT environment are subpar, then this type of architecture could potentially lead to infections in the most critical part of the network.

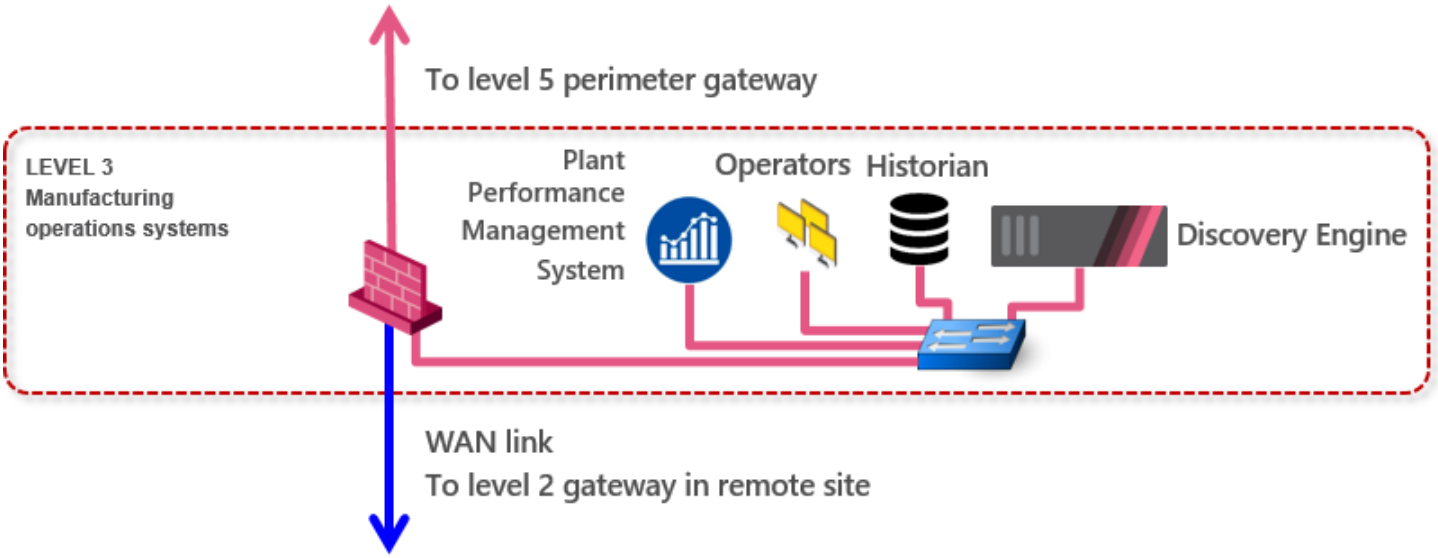
Recommended Security Controls:
To ensure maximum availability of the remote access gateway, allowing for third parties to remotely manage and monitor the OT equipment, it is vital to protect the gateway with an anti-DDoS solution (preferably on premises and cloud-based). In this blueprint, there is a jump server in the industrial DMZ. The VPN remote access server (RAS) sessions are terminated on the perimeter gateway in level 5. The gateway terminates VPN traffic, scans it for malware and only allows RDP traffic to the jump host. The jump host is then used to connect to operator workstations in level 2 for remote maintenance work. This approach is much safer than allowing inbound L3 VPN connections from the internet straight into level 2 and dramatically reduces the risk of the OT network becoming infected due to unsafe RAS connections originating from third parties. The jump server itself is protected by the gateway, which will only allow inbound RDP and has the necessary security controls enabled such as IPS, Anti-bot and application control.



Time	Service	Application Name	Primary Category	Access Rule N...	Resource
15 Sep...	ICCP (TCP/102)	MMS Protocol - Initiate Response	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	MMS Protocol - GetNamedVariableListAttributes Response	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	MMS Protocol - GetNamedVariableListAttributes Request	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61850 - GetDataSetDirectory	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61850 - GetLogicalDeviceDirectory	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61850 - Power cable LN GetDataDirectory/GetDataDefinition	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61400 - Wind Turbine Yawing Information GetDataDirector...	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61400 - Wind Turbine General Information GetDataDirecto...	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61400 - Wind Turbine Transmission Information GetDataDi...	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61400 - Wind Turbine Transformer Information GetDataDir...	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61400 - Wind Turbine Tower Information GetDataDirectory...	SCADA Protocols	Cleanup rule	
04 Sep...	ICCP (TCP/102)	IEC61400 - Wind Power Plant Reactive Power Control Informa...	SCADA Protocols	Cleanup rule	

An example of the log files generated by the SCADA-specific application control policy

Level 3: Manufacturing Operations Systems

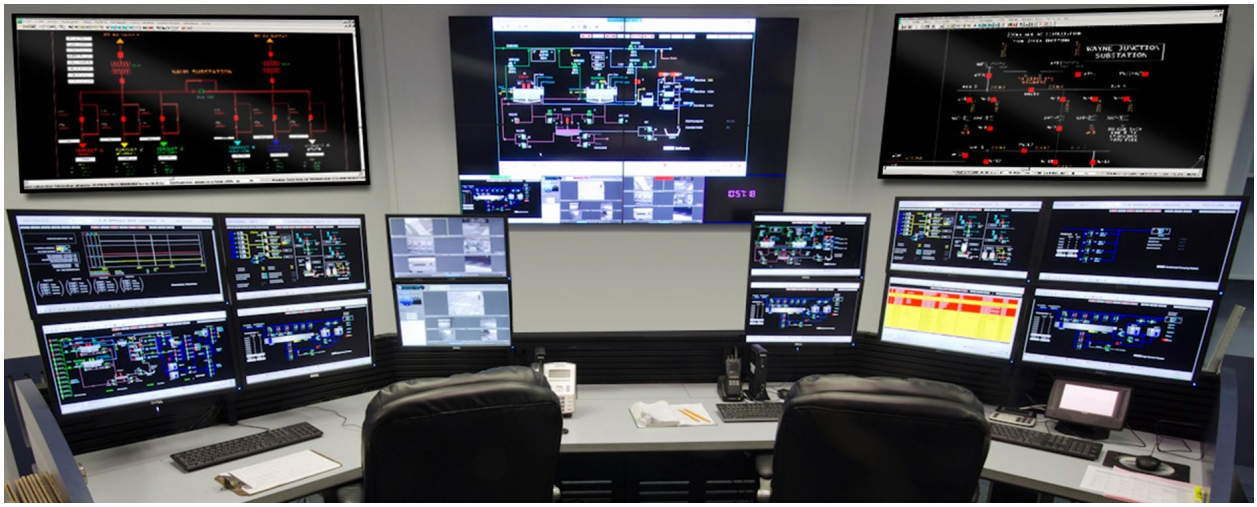


The security gateway in level 3 segments the IT from the OT part of the network and micro-segments level 3 itself. The plant management system, the operators, and the historian should all go in separate VLANs, while the gateway controls who is allowed to talk to who.

Systems and Processes:

In level 3, the manufacturing and operations systems are found, such as SCADA servers, Historian, Engineering stations, as well as the 3RD PARTY DISCOVERY ENGINE server (on a dedicated VLAN depicted on the right hand side of Level 3)

This is the place where operators are monitoring the industrial process 24/7 and adjusting it when required. Operators in this segment of the network can access the PLCs and RTUs in level 1. This is what the control room typically looks like:



In this area of the network, there is no need for ruggedized hardware anymore, regular 19' racks are used here.

Attack Vectors:

- Ransomware on Endpoints, machines being abused for cryptocurrency mining, bot infections, phishing via Email.
- Bot infections of the operator workstation could lead to sabotage of the industrial process.
- Unsecured USB ports.

Industry Examples:

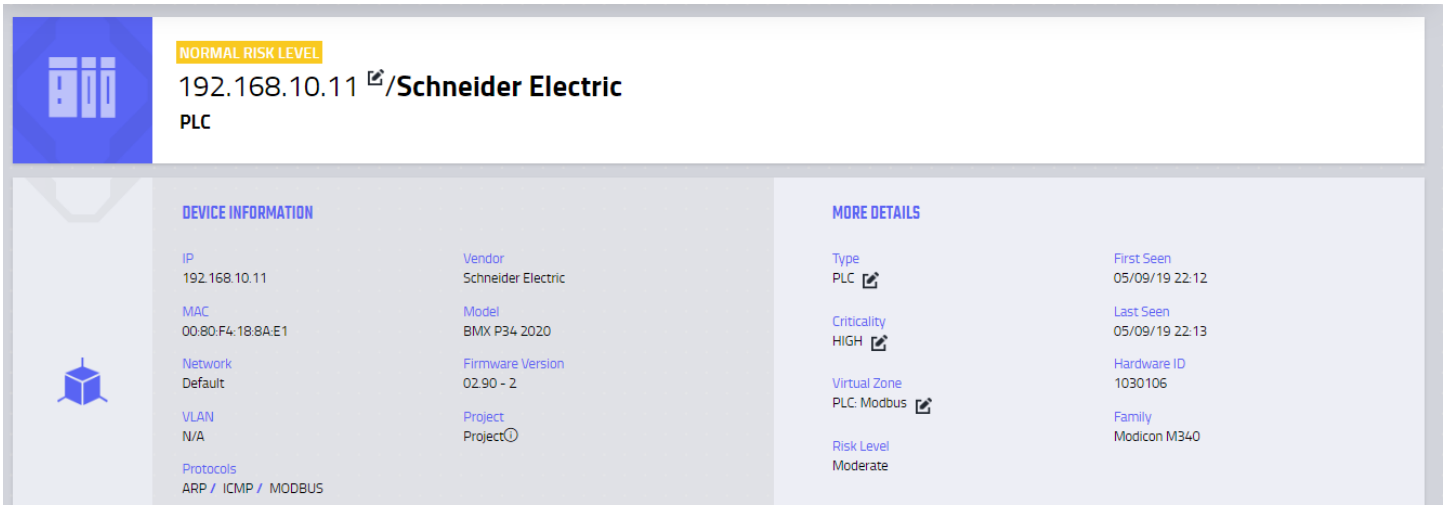
An unnamed petrochemical plant in Saudi Arabia was hit by triton malware in the summer of 2017. The hackers had deployed malicious software, or malware, that let them take over the plant's safety instrumented systems. These physical controllers and their associated software are the last line of defense against life-threatening disasters. They are supposed to kick in if they detect dangerous conditions, returning processes to safe levels or shutting them down altogether by triggering things like shutoff valves and pressure-release mechanisms. The malware made it possible to take over these systems remotely. Had the intruders disabled or tampered with them, and then used other software to make equipment at the plant malfunction, the consequences could have been catastrophic.

Risks:

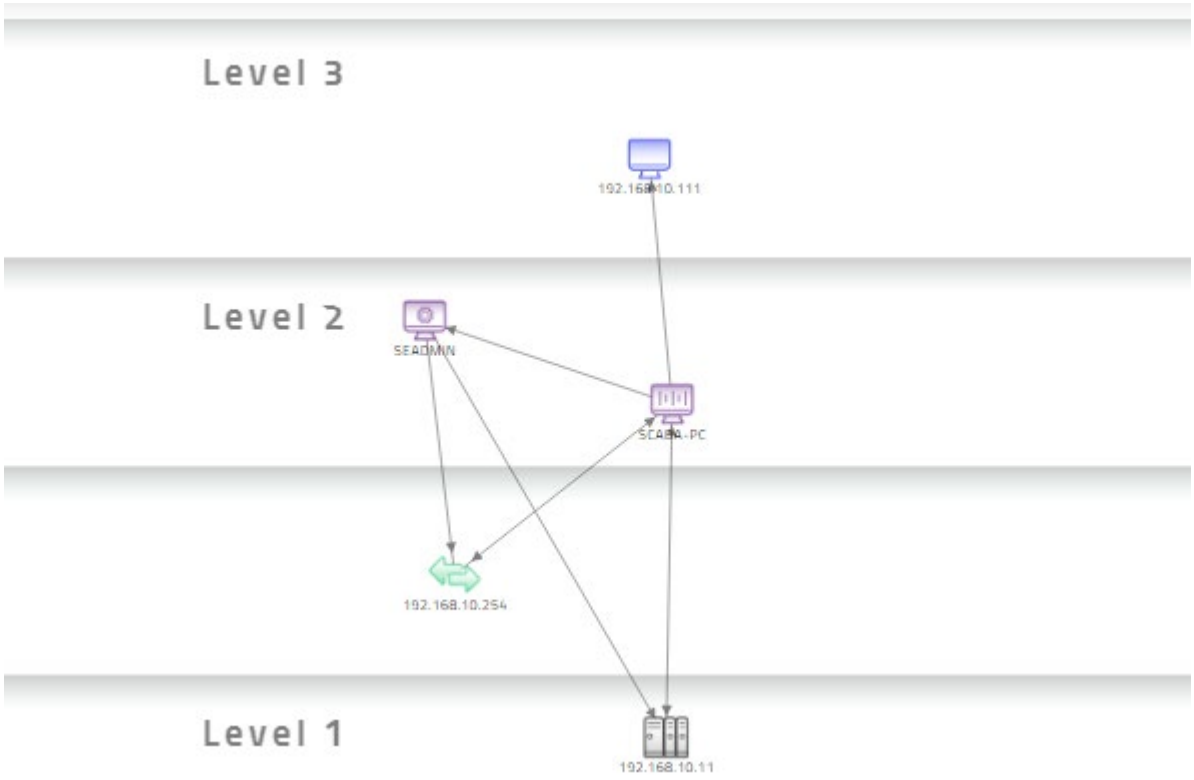
- Unwanted modifications to the industrial process
- Sabotage
- Industrial espionage
- Unpatched monitoring systems
- Lack of visibility into what kind of equipment is in place and if it is running vulnerable firmware

Recommended Security Controls:

- Anomaly and Asset detection and visibility
- Anti-bot
- IPS (typically used as a virtual patch to protect the monitoring stations of the operators)
- Sandboxing technologies to prevent Zero-day attacks (Check Point SandBlast)
- An application control security policy that only allows specific authorized commands to be sent from the operator workstation to PLCs.
- The use of Identity Awareness can add an extra layer of security to the policy by only allowing authenticated users, i.e. operators, to send specific commands to devices in Level 2.
- Encryption of the control traffic between operators in L3 and PLCs in L2 using IPsec to prevent eavesdropping and traffic replay attacks.
- Endpoint protection including Port Protection



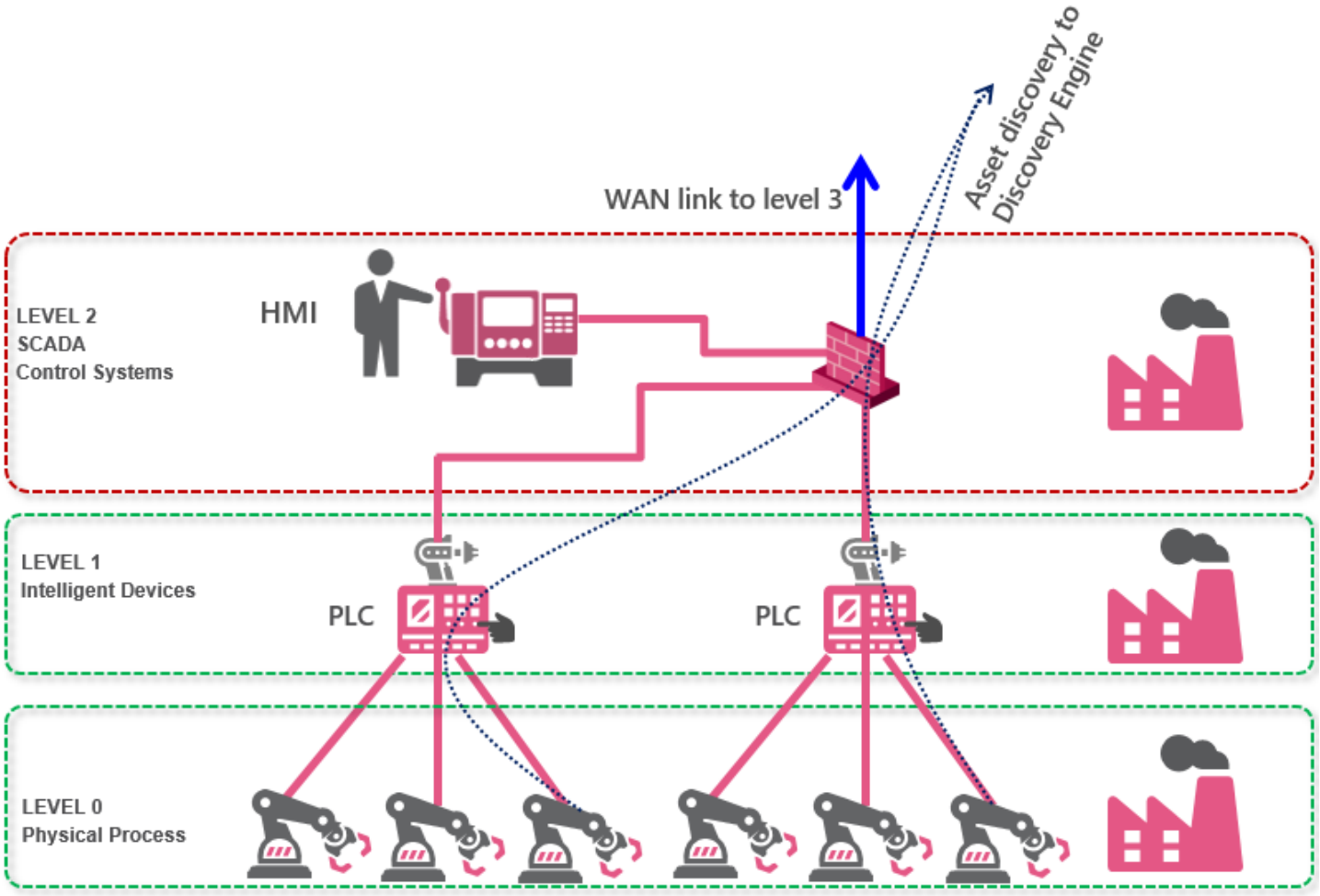
This screenshot from the Claroty console shows the kind of information can automatically be harvested about devices in levels 2 to 0.



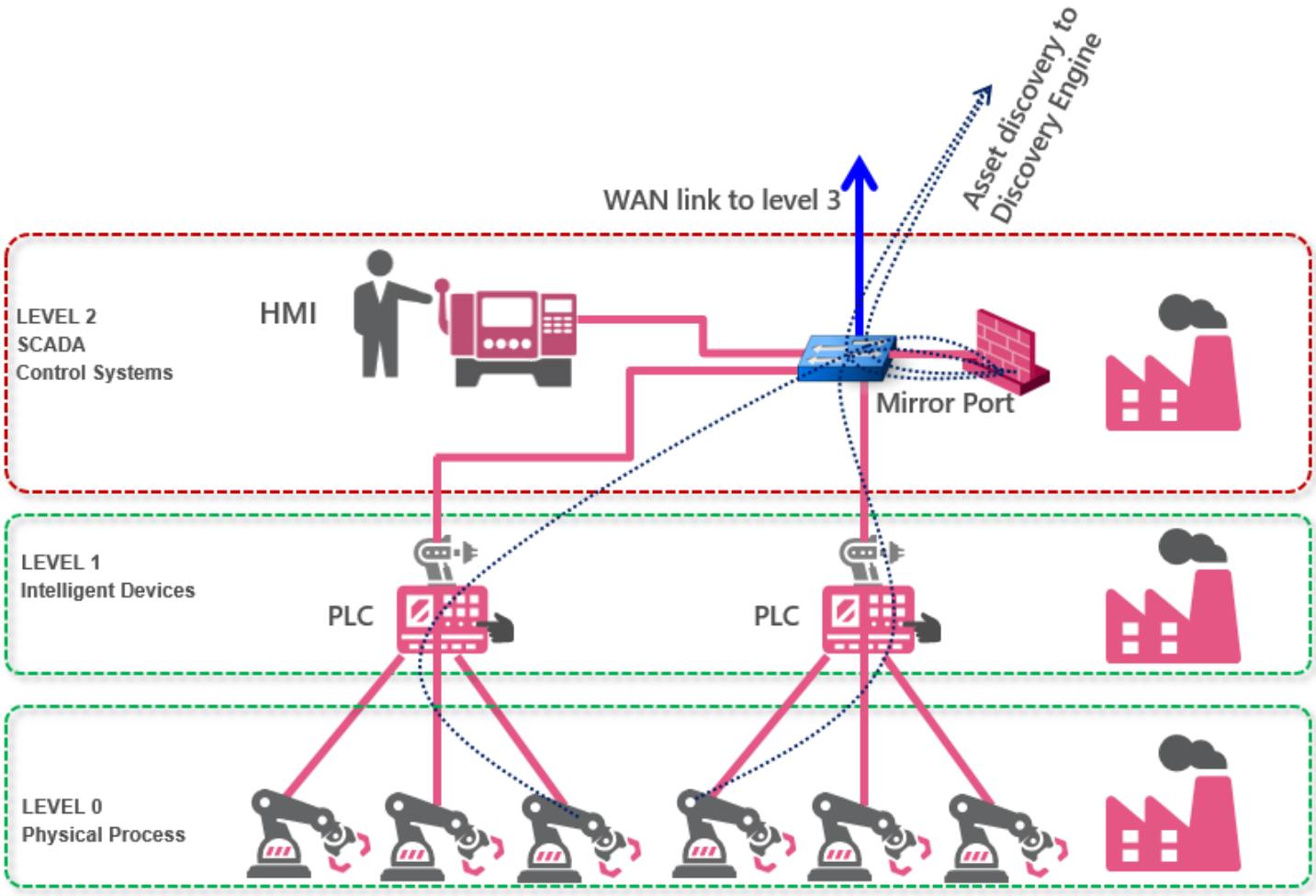
A second screenshot from the Claroty console showing where the discovered devices are situated according to the Purdue model.

Level 2 and 1: Securing Communications Between Levels

In example A, there is an inline gateway securing the communication between the local operator workstation and the different PLCs in different production lines. This is the recommended architecture as the gateway is not only able to detect, but also block unwanted traffic.



In this example B, the security gateway is connected to a switch via a mirror port (SPAN). From a visibility point of view, there is no difference between the previous example and this one. From a security point of view, there is. This gateway is unable to block unwanted traffic, it can only alert. A significant amount of companies still prefer this approach because in OT environments, blocking legitimate traffic is something that needs to be avoided at all cost and the chance of a false positive due to a configuration mistake or human error is still a possibility.



Systems and Processes:
The communication between level 1 and 2 is at the heart of the ICS network. This is where HMIs and PLCs are communicating using SCADA protocols and engineering traffic is sent to PLCs. While offering a security solution, we have to take into consideration latency issues, uptime of production equipment, processes and the sensitivity to any change which might affect the production.

Therefore, for most organizations, the most desirable security architecture is passive and non-intrusive. It is possible to use the gateway that separates Level 1 and Level 2 in mirror port mode and be passively listening and communicating back to the Claroty Discovery Engine in Level 3. However, from a security point of view, it is strongly recommended to segment Level 1 (and Level 0) from Level 2 by connecting them to different interfaces on the gateway that connects to the upper level (example A).

In case Level 2, 1 and 0 are all located in a remote facility, then the ruggedized gateway can communicate with the level 3 over IPsec VPN, MPLS, cellular or broadband. It is possible to deploy these gateways in High Availability as well and have them take care of dynamic routing.

In case of a single facility with multiple production lines, it is recommended to micro-segment level 2 and one with a gateway per production line as depicted in the first drawing above.

Attack Vectors:

- Denial of Service exploitation on HMIs, RTUs, IEDs or PLCs
- Exploitation of known vulnerabilities of HMIs, RTUs, IEDs or PLCs
- The use of unencrypted protocols leaves this segment vulnerable to sniffing, allowing hackers to figure out passwords and use traffic replay attacks with modified payload data
- Some intelligent devices have hardcoded passwords, and some admins do not even bother to change the passwords of intelligent devices, even if it is possible.
- Patching systems in this layer is often not done as the main focus is uptime, instead of security leaving both the application and the OS vulnerable
- Vulnerable machines in level 1 are often targets for hackers to use as crypto miners or for ransomware
- Malware able to send malicious commands to a PLC jeopardizing the industrial process

Industry Example:

July 2nd, 2019: Schneider Electric released a CVE describing vulnerabilities in their Modicon controllers. Successful exploitation of this vulnerability could result in a denial-of-service condition. The CVE states the following: To mitigate risks associated with this Modbus vulnerability, users should immediately set up network segmentation and implement a firewall to block all unauthorized access to Port 502/TCP.

Risks:

- Unwanted modifications to the industrial process
- Sabotage
- Industrial espionage

Recommended Security Controls:

- Use gateways running IPS to protect vulnerable systems as a virtual patch instead of patching the actual systems, causing downtime. A screenshot of such configuration is shown below:

No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On
1		[Type] Endpoint	N/A	Optimized	Log Packet Capture Forensics	gw-05f13a
2		[Zone] PLC: Modbus	N/A	Strict	Log Packet Capture Forensics	gw-05f13a

- The communication between level 2 and 3 can be encrypted using IPsec to protect sniffing and replay attacks.
- A security gateway can be connected to a mirror (SPAN) port on a switch in this level, operating as a sensor, feeding information about asset discovery and anomaly detection to the Claroty Discovery Engine.
- Customers willing to consider inline security gateways in level 1 could separate local operator workstations and HMIs from PLCs and RTUs ensuring no unauthorized commands can be sent to them. When using a gateway connected to a mirror port, this can also be detected, but not prevented. An example of such an application control policy is shown below:

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1		[Type] Endpoint	[Type] PLC	Any	Modbus Protocol	Drop	Log Mail Accounting
2		[Type] HMI	[Type] PLC	Any	Modbus Protocol	Accept	Log Alert Accounting

- Endpoint security can be considered on machines with supported operating systems.
- Appropriate L2 security on switches
- Consider the use of an out-of-band network solely used for management traffic, signature updates and firmware updates of equipment in this level. Only SCADA protocols should be seen in Level 1.

- Do not allow remote technicians to directly connect to the level 1 network, prefer the use of a jump host in the DMZ in level 3.5: When unmanaged assets connect to this network, the security posture is unknown and can therefore not be trusted.

Level 0: Physical Processes

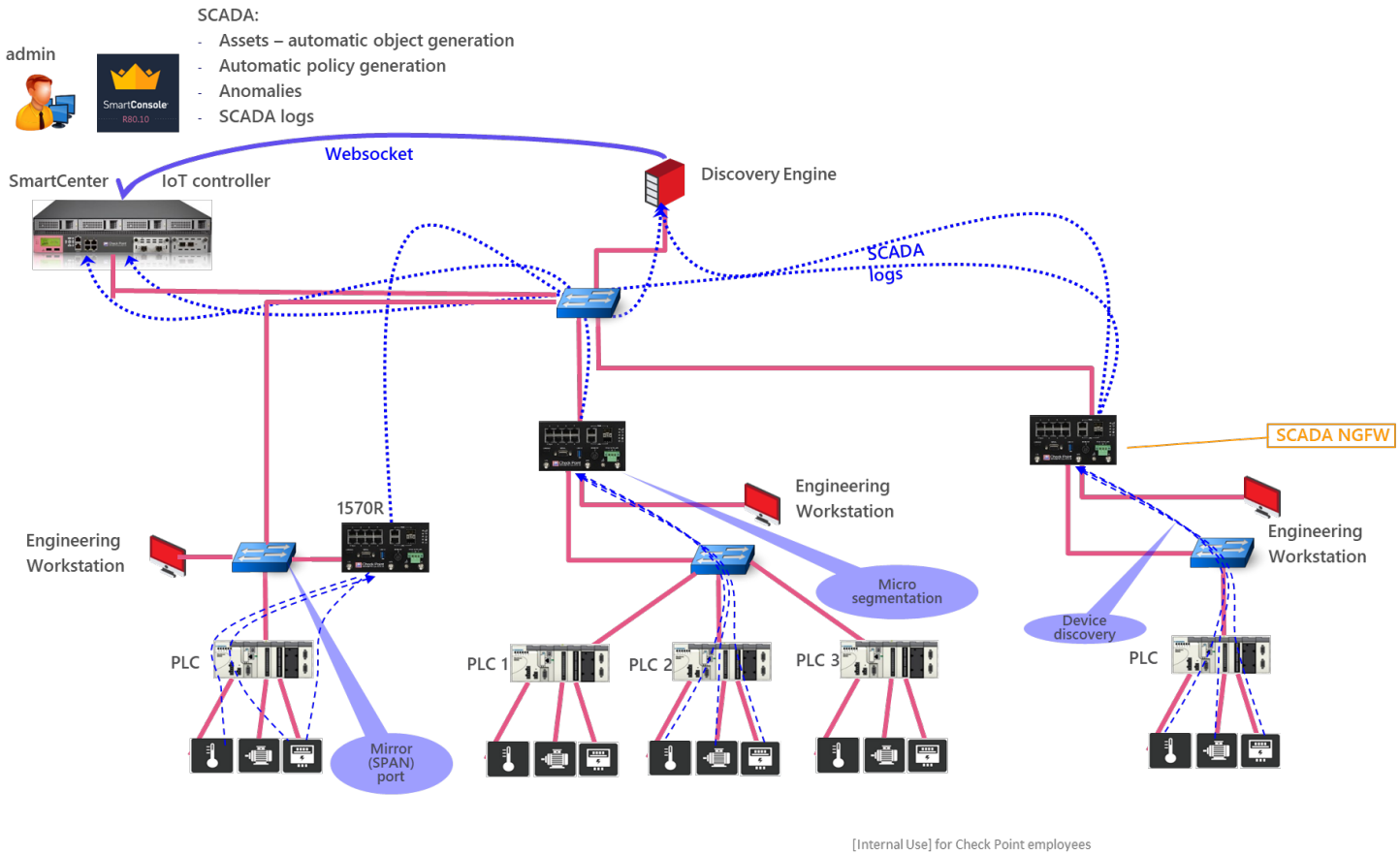
Systems and Processes:
This is where the physical process is taking place. Here we find field devices that communicate with intelligent devices in level 1. The devices in level 0 are not intelligent; field devices can be valves, sensors, actuators and so forth. Some of them are active like a valve, some of them are passive like a temperature or pressure sensor.

Attack Vectors:
As long as the field devices in level 0 are directly connected to the PLCs or RTUs in level 1 using analog links, the likelihood of a cyber-breach occurring here is fairly low. In case something would go wrong, it would most likely be due to a physical security breach. In case the field devices are connected to level 1 using IP and switches are involved, security controls between the 2 levels are recommended. The purpose here would be to have an additional pair of eyes. For example: if a PLC receives an instruction from level 3 and sends it down to a field device in level 0, there should be consistency.

Risk:
Disruption or modification of the physical process.

Recommended Security Controls:
It is recommended to use point to point connections between the intelligent devices in level 1 and the field devices in level 0. In case the communication between level 1 and level 0 is done over IP, prefer point to point connections. If point-to-point links are not possible and Ethernet switches are used in level 0, ensure the appropriate L2 security is enforced: admin down of all unused switch ports, MAC authentication on used switch ports, consider the use of additional security gateways between Level 1 and Level 0. The use of a trusted baseline policy with application control can warn an admin if an unknown command is sent to a field device.

ARCHITECTURE AND COMPONENTS SUMMARY



1. **Discovery Engine: Asset and Anomaly Detection (depicted in red on the right hand side)**

The Discovery Engine that ensures asset management and anomaly detection for ICS networks provides rapid and concrete situational awareness through real-time alerting.

The Discovery Engine software is installed on a server or runs as a virtual machine (VM). The system connects to Check Point security gateways and managed switches. Employing deep packet inspection (DPI) on a real-time copy of network traffic, the system uses a safe, fully passive approach that never impacts industrial control systems or the safety and reliability of the process.

When connected to an industrial network using Check Point gateways as sensors, The Discovery Engine automatically discovers assets, learns network topology, models the network's unique communication patterns and creates a fine-grained behavioral baseline that characterizes legitimate traffic. The system provides important insights about network hygiene, configuration issues, and vulnerable assets.
Depending on the 3rd party discovery engine's method of information gathering, a Check Point gateway can be used as a sensor, a 3rd party sensor can be used, or the information can be obtained from a mirror port on a switch.

Following the learning period, the system shifts to operational mode where alerts are triggered for any violation of the baseline. The Discovery Engine generates actionable alerts that are clear, consolidated, and context-rich. This provides security and control teams rapid situational awareness of potential and actual process disruptions, enabling teams to quickly and efficiently respond to events as well as maintain the safety and reliability of industrial processes.

2. Security gateways (depicted at the bottom with SCADA NGFW caption)

In the Claroty example, the Check Point security gateway operates as a tcpdump-like sensor for SCADA device discovery and anomaly detection in the subnet/broadcast domain it resides in. This information is then sent to the Claroty Discovery Engine. Multiple networks or VLANs can be monitored by spanning the traffic to a mirror port on this gateway, as depicted by the gateway in the middle at the bottom of the picture. Multiple PLCs in different VLANs can be connected via a switch to the gateway using an 802.1q trunk. The gateway can apply policies between the VLANs and can sniff traffic in all VLANs for device discovery. The security gateways serve multiple purposes, depending on the way they are deployed.

When inline (depicted at the bottom right):

- To segment the different zones or even microsegment within one zone.
- To secure the communication between the different segments using firewall access rules, intrusion prevention (IPS) and application control to filter on specific SCADA commands and parameters.
- To generate logs that will be displayed in an intuitive way on the management station.
- To operate as a sensor in zone 1 and 2 to feed information about the assets back to the Claroty Discovery Engine.

This mode is active, meaning the gateway can effectively block unwanted traffic (PREVENT MODE).

When connected to a mirror port with one single interface (depicted at the bottom left):

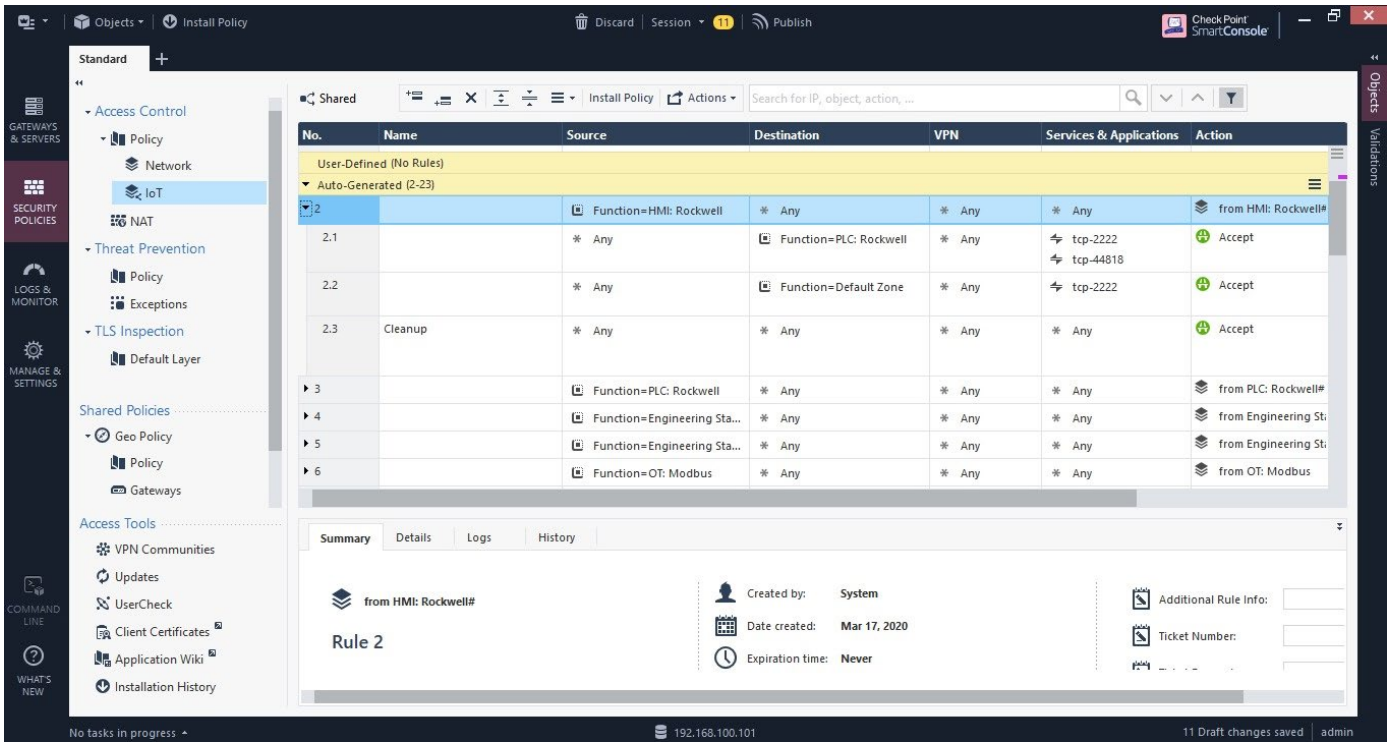
- To sniff the traffic it sees and to generate logs that will be displayed in an intuitive way on the management station and on the Claroty Discovery Engine.

This mode is passive, non-intrusive and easy to deploy. However, the gateway can neither take action nor block unwanted traffic (DETECT MODE)

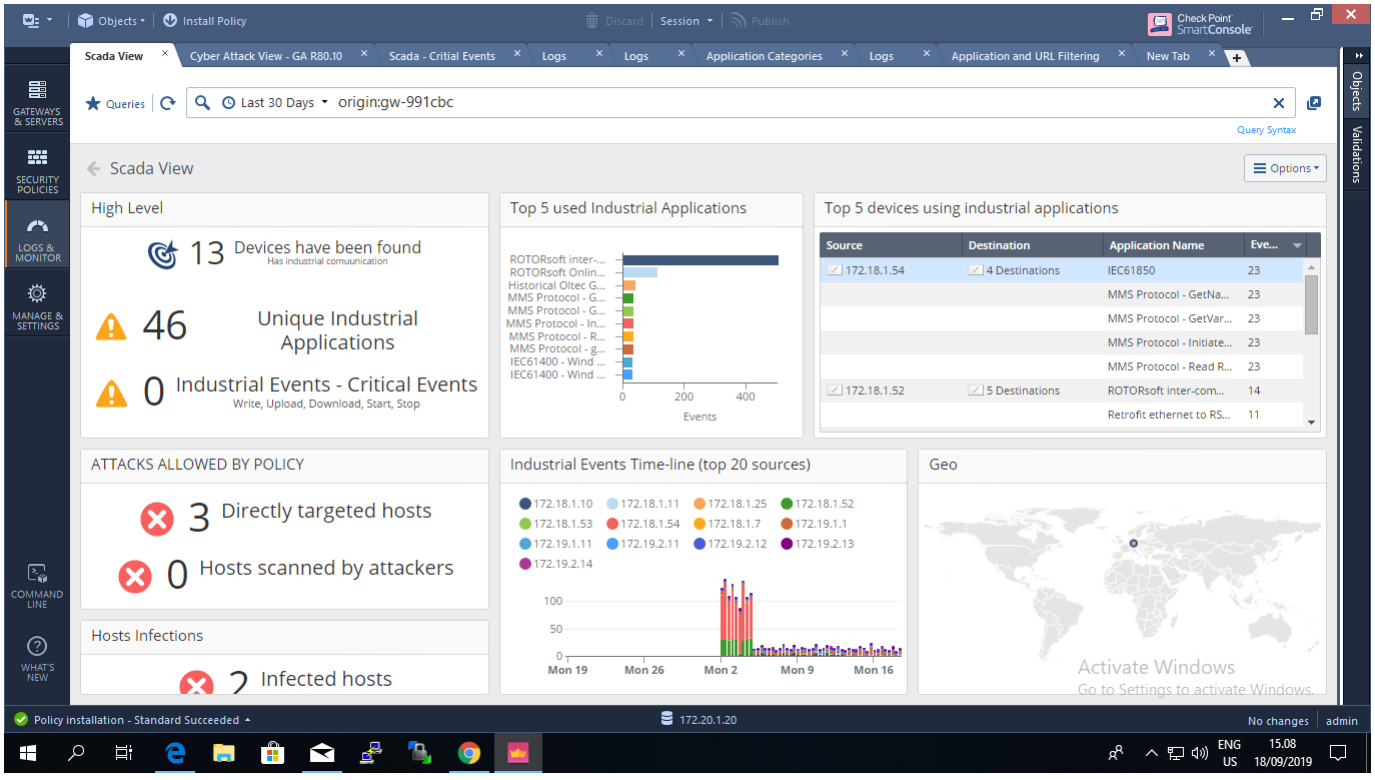
3. The management station (depicted at the top left)

The Security Management server is used to:

- Push policies to all gateways in the network.
  - A new layer in R80.40 management, called IoT Controller, is managing the communication with the Discovery Engine using API's.
- The IoT controller:
  - Automatically create objects for all the assets identified by the Discovery Engine
    - Policies and logs are textual (easy to read and understand)
    - No more logs and policies with IP addressed, but real object names
  - Assets groups are created
  - Adaptive policy that changes based on asset's real-time behavior and risks
  - Discovery Engine recommended policies are supporting policy decisions
  - Easy to define new policies to better enforce the ICS network

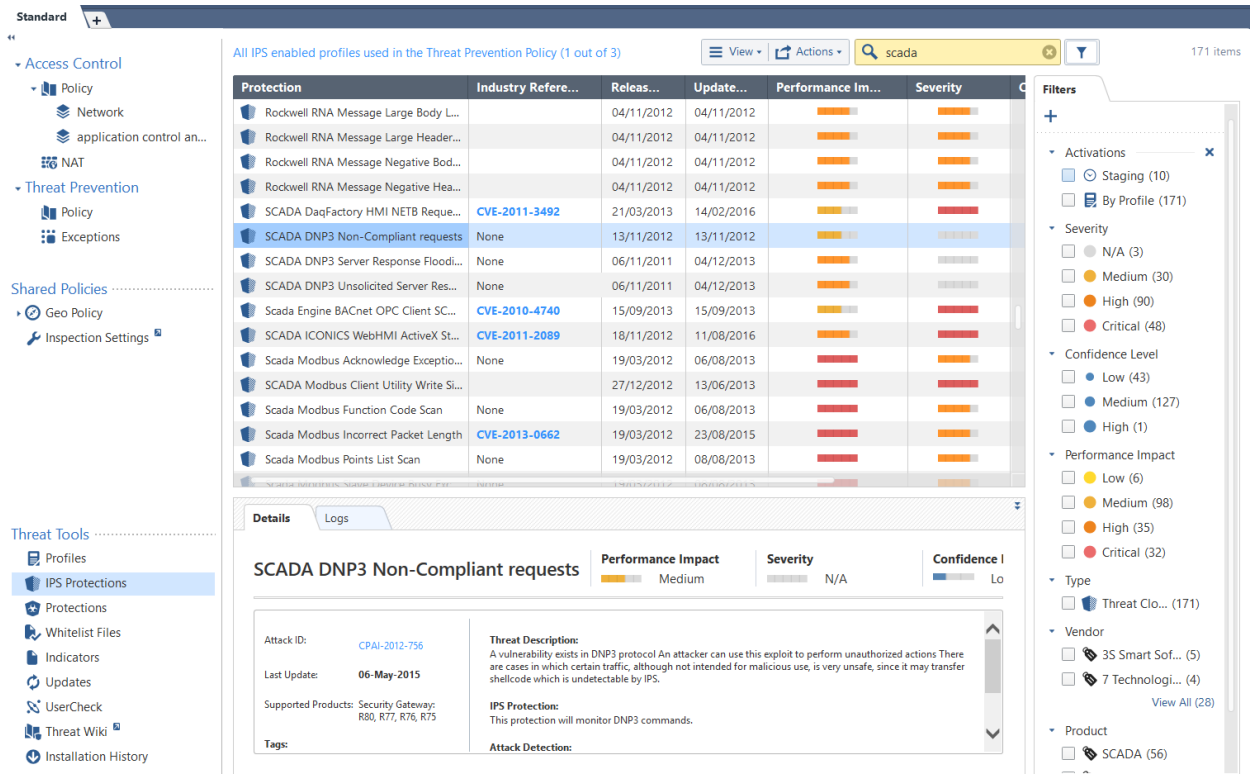


- Receive log files from all the gateways it manages and display them in an intuitive way. (see screenshot below)



5 KEY TAKE AWAYS

1. Ensure proper segmentation is in place. Remember that this is not about having a lot of different VLANs and / or subnets and then just enabling routing between them. It is about having the correct security controls in place and enabled between the segments.
   To recap: Sandboxing technologies at the perimeter (level 5), including SSL/TLS inspection. On internal segments (level 4 and below), Firewall, IPS, Identity Awareness and Application Control should be the minimum. Sandboxing is vital to protect against zero-day attacks, a common attack vector used by hackers to target critical infrastructure.
2. Threat Prevention is vital. Detection only informs you when the damage has already been done.
3. The IPS blade contains several signatures that are specifically aimed at securing ICS environments. Enable IPS in prevent mode wherever possible and make sure to specifically monitor alerts for these signatures.



4. Application control supports several SCADA protocols up to command-level and even parameter-level. This allows for the creation of a security policy that authorizes only specific commands to be sent to PLCs and deny everything else.
5. Visibility is key to security. Ensure there is enough man power to monitor the environment. Tools like SmartEvent, 3rd party Discovery Engine and a dedicated SIEM can reveal a lot of information that may otherwise go unnoticed.

REFERENCES

[1] The Norsk Hydro cyber attack is about money, not war, https://www.wired.co.uk/article/norsk-hydro-cyber-attack
[2] Forrester Research, Five Steps to a Zero Trust Network, December 14 2017, https://www.forrester.com/report/Five+Steps+To+A+Zero+Trust+Network/-/E-RES120510
[3] Industrial Cybersecurity, https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems
[4] What was that Purdue Model stuff, anyway?, http://scadamag.infracritical.com/index.php/2018/03/01/purdue-model-history/