WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

Implementing a Defensible Architecture

Using OT Asset Visibility and Firewalls to Protect Industrial Operations

BASED ON THE JOINT WEBINAR: IMPLEMENTING A DEFENSIBLE ARCHITECTURE IN THE POWER INDUSTRY: HOW PALO ALTO NETWORKS AND DRAGOS EMPOWER YOUR ICS/OT CYBERSECURITY JOURNEY

DRAGOS, INC.

SEPTEMBER 2023

paloalto NETWORKS

Digital transformation is bringing about the convergence of IT systems, industrial control systems (ICS) and operational technology (OT). Companies are embracing it as a way to streamline operations, improve efficiencies, and identify new opportunities. But that process also means the danger of introducing new cybersecurity threats into IT ecosystems increases significantly. Those risks come from a range of factors, including remote access, shared credentials, and unchecked communication to critical ICS/OT assets that may not be protected by proper network segmentation.

According to the **Dragos 2022 ICS/OT Cybersecurity Year In Review,** 50 percent of Dragos services engagements involved issues with poor security perimeters. Dragos analysts speculate the improvements here are a result of increased awareness that proper segmentation is an essential aspect of a defensible architecture.

The SANS Institute has identified five critical controls that are needed to implement robust ICS/OT cybersecurity. They include:

- Having an ICS incident response plan.
- Implementing a defensible architecture.
- Enabling ICS network visibility and monitoring.
- Securing remote access.
- Practicing risk-based vulnerability management.

Establishing a defensible architecture is crucial to be able to monitor for anomalous or concerning events and actions, detect and defend against active threats, and mitigate any impacts on the overall operation. The key components of a defensible architecture include: OT network visibility, identification, and asset inventory at critical sites to enable utilities to understand their existing network architecture, and better segmentation to allow security teams to more easily prioritize, investigate, and respond to threats that could otherwise move unchallenged laterally through the network. These steps are all designed to ensure the uptime, resilience, and safety of utility assets and personnel.

Challenges for Building a Defensible Architecture

Many of the challenges faced by the electric utility industry are common throughout the industrial sector. This includes a reliance on legacy OT that was never designed to be connected to outside systems. Those systems are also often built in isolated locations or harsh working environments, and yet require continuous operations.

86% of Dragos services customers in the electric industry had **limited to no visibility** into their ICS/OT environment.

— DRAGOS 2022 ICS/OT CYBERSECURITY YEAR IN REVIEW

Many utilities have little to no visibility into their OT assets, how they are performing over time, or what they are connected to. Even OT communication from devices is likely to be one way. Many OT devices can provide a stream of information, but are unable to receive any instructions, instead requiring on-site input to change their behavior or settings.

These are long-standing characteristics of the electric utility industry. But the industry itself is facing new

challenges, specifically the push to transition to decarbonized energy. In the past there was a natural segmentation – thermal carbon-based sources typically were hosted in large physical locations. Whether oil-fired or coal-fired power stations were used to generate electricity with limited security only required protecting the physical perimeter around the facility because of limited connectivity to these systems.

But because the industry cannot just automatically build new transmission or distribution infrastructure, it has to become more reliant on digital technologies to more efficiently transmit and distribute electricity. The industry is seeing a lot of network redesigns taking place; these networks once were flat with little connectivity to anything other than internal systems, but today on-site and remote workers are using remote access connections to transfer information.

> One of the things that's allowed us to interconnect all these devices together is the move towards standardized protocols, enabling multi-vendor installations. Interoperability is speeding up digital adoption, but it also means that we lose that security by obscurity.
>
> **— PHIL TONKIN —**
> Chief of Staff, Dragos

Integrating IT and OT environments introduces many new cyber risks and challenges. The two threat vectors we are seeing most in electric utilities are advanced persistent threats (APTs) and ransomware. Out of the 21 threat groups Dragos tracks, 17 of them target the electric sectors, which illustrates how the threat landscape is growing and the capabilities are adapting.

Until recently, the impact of threats like ransomware has not been very big in the electric utility industry because existing IT/OT connectivity has been limited to necessary operations that have been in place for quite a while. But the potential benefits of digital transformation, including efficiency and cost savings, are creating pressure to further integrate the two types of systems.

In an IT environment, cyber attacks do occur frequently, but systems administrators know that vigilance is needed, and over the years tools and tactics have evolved to help protect IT from critical vulnerabilities. They employ identity management, monitoring and validation of online traffic contents, and use tools like machine learning to map system behaviors and flag sudden or unexpected changes. On the OT side, few native protections exist, which makes creating a blended OT/IT environment a potentially serious endeavor that can greatly expand the attack surface.

How can electric utilities implement segmentation without disruption of operations? In distribution environments, the perimeter typically sits above the Control Center, and there is implicit trust between the control centers and most substations without a lot of segmentation. As organizations introduce additional monitoring and segmentation, it also creates a critical need for more routable traffic.

But the good news is, all of these challenges can be managed to mitigate the increased risks of a blended OT/IT environment.

How to Build a Defensible Architecture

As noted above, implementing a defensible architecture is the second control that organizations must consider. A defensible architecture is defined as an architecture that reduces as much of the agreed-upon risk as possible through system design and implementation, while also simplifying the efforts of human defenders.

The common attributes of good defensible architectures include:

- Having accurate asset identification and a device inventory.
- Segmenting environments wherever possible.
- Determining when and where bi-directional access is needed.
- Having the ability to collect network traffic and systems communications.
- Having a log collection from systems of value.
- Being able to quickly shift into a "defensible cyber position" in response to threats.

Achieving Accurate Asset Visibility for the Crown Jewels

The first key attribute of any defensive architecture is asset visibility – knowing what is important, the **crown jewels** that an organization can't exist without, and how to protect those assets. This includes recording important information about each system such as the software version it is running, its physical location, the owner of the asset and how critical it is to overall operations. With good asset visibility and inventory, utilities can understand what their normal operations baseline look like, identify rogue/unrecorded assets, detect threats with a high signal/low noise ratio (cutting down on false alerts), and identify and visualize asset relationships and communication pathways. This step is essential, both because it provides the starting point to understand the ramifications of those communications being impeded and as the building block for network segmentation.

> Your first step to understanding your environment is having a good asset inventory and good asset visibility. Having this baseline, knowing what is normal in your environment is crucial.
>
> — JOSE AVILA-GOMEZ —
> Senior Industrial Consultant, Dragos

Segmenting the Environment

The second attribute, being able to segment the environment, means determining what needs to be isolated. Start from that point because if something is defined as critical or crown jewels, anything that touches it upstream also becomes critical.

The value of segmentation is in breaking an entire system into smaller protective zones and reducing ingress and egress into as few pathways as possible, to create intentional bottlenecks for a next-generation firewall to provide enhanced security and monitoring.

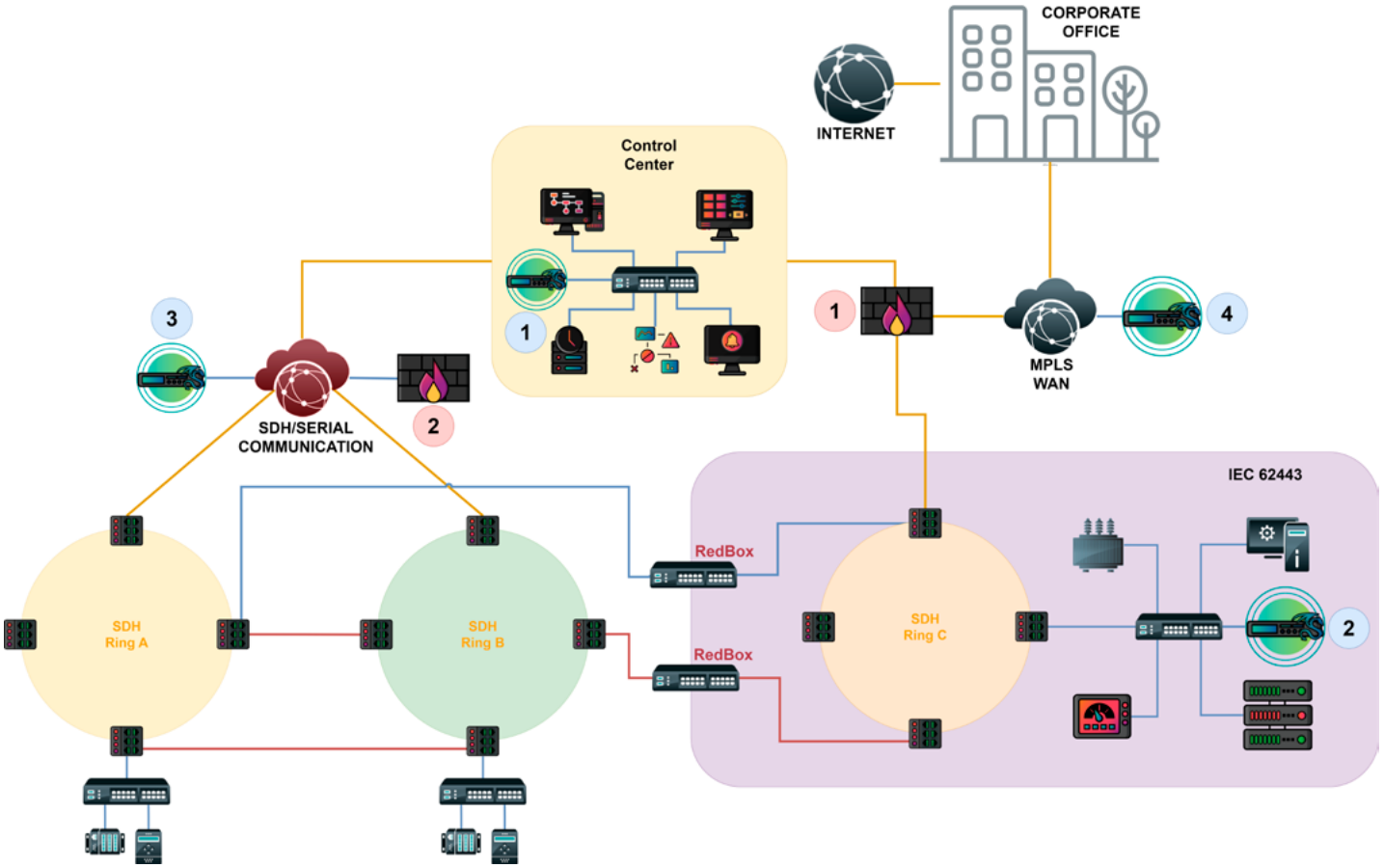


Diagram 1: Representation of a segmented network utilizing The Dragos Platform and Palo Alto Networks Next-generation Firewalls

Part of the power of segmentation is being able to enforce it – not just who gets access to each ICS/OT device, but also under what circumstances. For example, factors such as the time of day, where communications may originate or be sent and why the device needs to communicate in the first place are all part of creating effective segmentation rules. Thus, part of segmenting the environment means establishing policies for accessing OT. Focus should be given to those assets that are critical, with security processes designed around them. Only the people who absolutely need access should be granted permission to interact with those assets. We call this process increasing the operational surface, because we recommend allowing only those services, people and products needed for a specific function or capability.

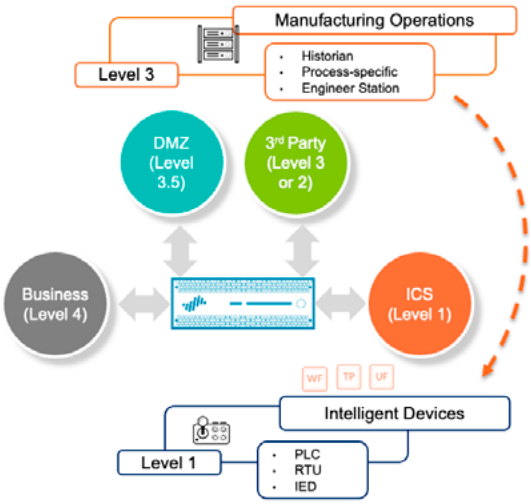
Dragos works with the Palo Alto Networks to help utilities isolate, identify, and group these critical assets in ways that are usually easily reversible in case they need to be changed. That is a major benefit in this environment, because maintenance windows are often very tight.

Enabling Bi-Directional Communication When Required

Bi-directional access is an important attribute to defensible architecture, by implementing least privileged access in a way that is minimally impactful to production and more importantly doesn't compromise safety of the operation.

Rather than implementing it everywhere, however, assets need to be evaluated based on whether they should have read-only communications or be upgraded to allow for remote access – now and in the future. Bi-directional access also fits into some of the segmentation decisions mentioned previously, since the purpose is to be able to identify, monitor, and control communications.

Who	User-ID	Process Engineer
What	App-ID	Modbus
When	Working Hours	Time based policy
Where	Zone/Enclave, Country Code	Level 3 to Level 1
Why	Read-Coils	Control, Data Gathering
How	Content-ID, Threat Prevention, URL Filtering, SSL Decryption, Wildfire	Allow



Policy Optimizer

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
1	Read-Coils	LessSecure-HighlySecure	universal	3rdParty, ICS-L3	any	Peter-ProcessEngineer	any	ICS-L1	any	any	modbus-base, modbus-read-coils	application-default	Allow	
2	Historian	HighlySecure-LessSecure	universal	ICS-L2	any	any	any	ICS-L3	any	any	opc-base	application-default	Allow	

Diagram 2: Example of policy creation for OT

Bi-directional access helps define what Palo Alto Networks consider the "protection surface," those assets that are critical, then designing security processes around making them available to the people and processes that need them. While many security professionals also refer to, "reducing the attack surface," it also makes sense to say, "increase the operational surface," as we are going to allow only those services, people, and products that are needed for that capability or function.

Collecting Network Traffic and Logs from System of Value

When the system has its firewalls in place, they provide complete visibility of traffic ingress and egress, the behaviors of personnel and what they are doing. These are what generate event logs.

Using log information productively starts with implementing a **collection management framework (CMF)**, which is a structured approach to identifying all data sources and determining what information can be obtained from each source. Many of the devices connected on networks can generate these logs, but having the framework in place will keep them from overwhelming the security operations center with too much data. When combined, the logs and the framework can provide an extremely granular picture of any incidents and responses can provide an extremely granular picture of any incidents and responses.

A collection management framework (CMF) is a structured approach to identifying data sources and determining what information can be obtained from each source.

- What information is available?
- Where does the data live?
- How is it accessed?
- How long is the data retained?

	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

Diagram 3: Sample CMF of a Hypothetical Electric Company

Implementing a Defensible Cyber Position

Here is the destination for all of this work – the ability to quickly shift into a defensible cyber position. In the event of a cyber incident, a utility can isolate operations and contain a breach to just one part of the system, so that if an attacker enters a utility's business systems, for instance, they can be isolated and disconnected from the ICS/OT devices running the generation plant or monitoring the transmission of electricity.

Now that cybersecurity is in place – firewalls, asset visibility and policies – if a workstation is compromised, an analyst will automatically receive an alert and that workstation can be isolated and quickly moved to a sandbox or an analysis group for further inspection while the rest of the operation continues to run.

Enhancing ICS/OT Security Perimeters

Dragos and Palo Alto Networks have teamed up to offer industrial organizations a defensible architecture that includes asset visibility, threat detection, and prevention technologies, enabling IT and OT professionals to improve facility operations while maintaining the availability of systems and protecting operations processes.

As a foundational complement to firewalls, the Dragos Platform, an industrial control system (ICS) cybersecurity technology, delivers unmatched visibility of ICS/OT assets and communications. It allows teams to rapidly pinpoint threats through intelligence-driven analytics to identify and prioritize vulnerabilities and provide best-practice playbooks to guide teams as they investigate and respond to threats before they cause significant impacts on an organization's operations, processes, or people.

The Palo Alto Networks Next-Generation Firewall (NGFW) offers a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations that focus on what matters and enforce consistent protection everywhere. ML-Powered NGFWs inspect all traffic, including all applications, threats, and content, and they tie that traffic to the user, regardless of location or device type.

Together, this solution protects OT assets from potential threats, helping segment industrial networks and build compliance with various industrial standards, regulations, and guidelines, such as NERC-CIP, ISA99/IEC62443, CFATS and ANSI/AWWA G430. This allows teams to capture the benefits of industrial digitization efforts across both IT and OT environments while being able to see risks, reduce attack paths, and secure a wider range of environments.

Scenario: Improved Asset Visibility for Better Firewall Policy

To see how Dragos and Palo Alto Networks solutions work together to isolate a threat and keep operations running, let's walk through a hypothetical threat scenario to understand how segmentation and visibility work together to identify the intrusion and automatically take action.

Assets can be grouped by properties, attributes, and parameters, and they are used to generate and populate asset profiles. When you define your enclaves and implement least privileged access based on the user, time of day or other factors, and set the level of protections that should be wrapped around user or device activities.

After the attributes have been configured, a list of assets matching the defined criteria is shown to the user before saving the asset sync profile. This list of assets can be exported and synchronized to address groups in Palo Alto Networks NGFWs for easier management by a firewall administrator who can then apply appropriate policies to any address groups as updated by the Dragos Platform.

In this scenario, a bad actor has gained access to the corporate network. Moving laterally through the network utilizing shared credentials, the attacker made their way toward the OT network. 54% of service engagements included a finding of shared credentials in OT systems, the most common method of lateral movement and privilege escalation, according to the **Dragos 2022 ICS/OT Cybersecurity Year In Review**.

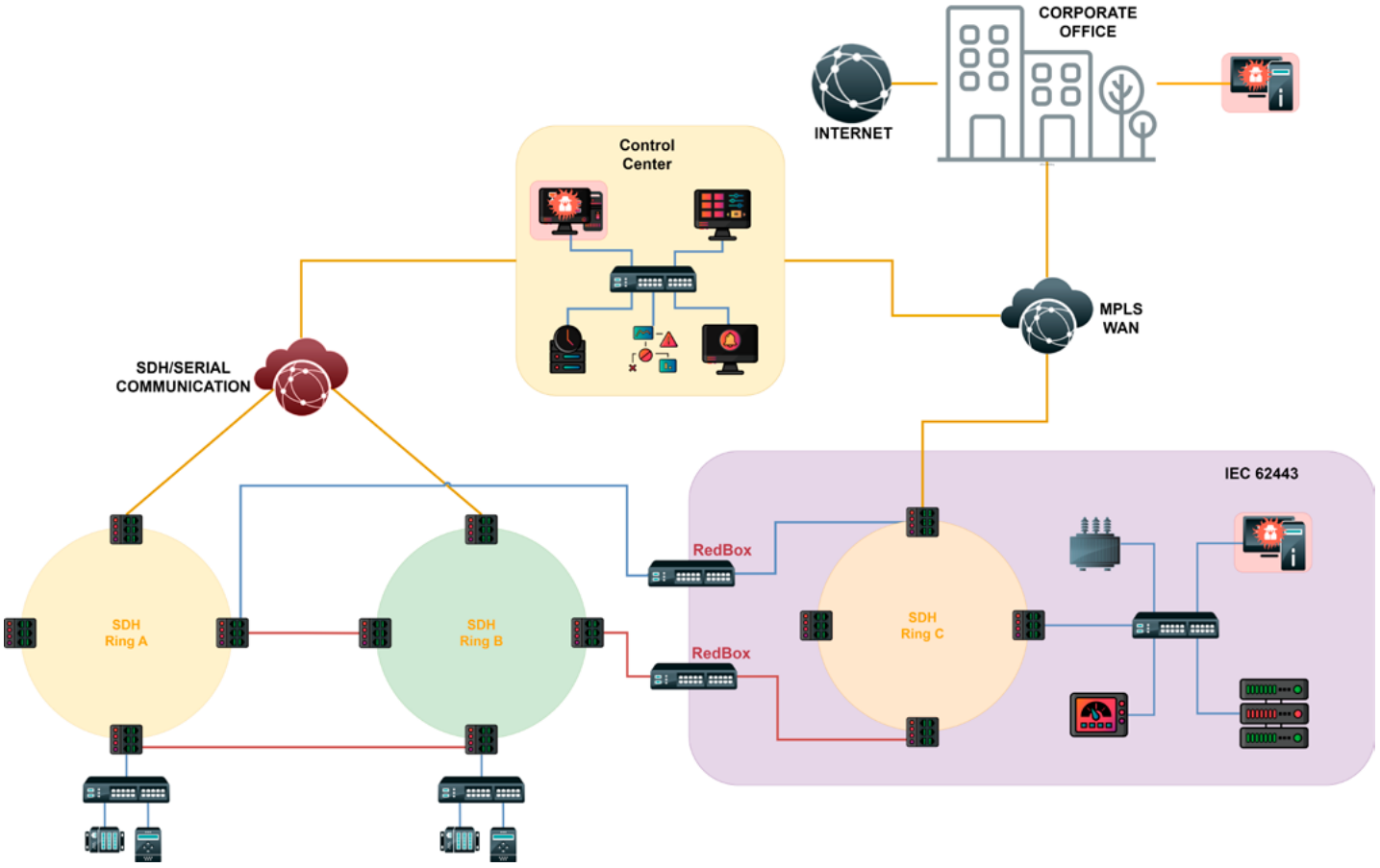


Diagram 4: High-level "flat network" connectivity between the Control Room, SCADA and different substations.

The SOC receives a Workstation Compromise Alert. The compromised asset is automatically assigned to an address group for further investigation and any other necessary actions in keeping with security policies. The workstation is prevented from communicating with the OT environment or receiving any communications from it.

Workstation Compromise Alerts

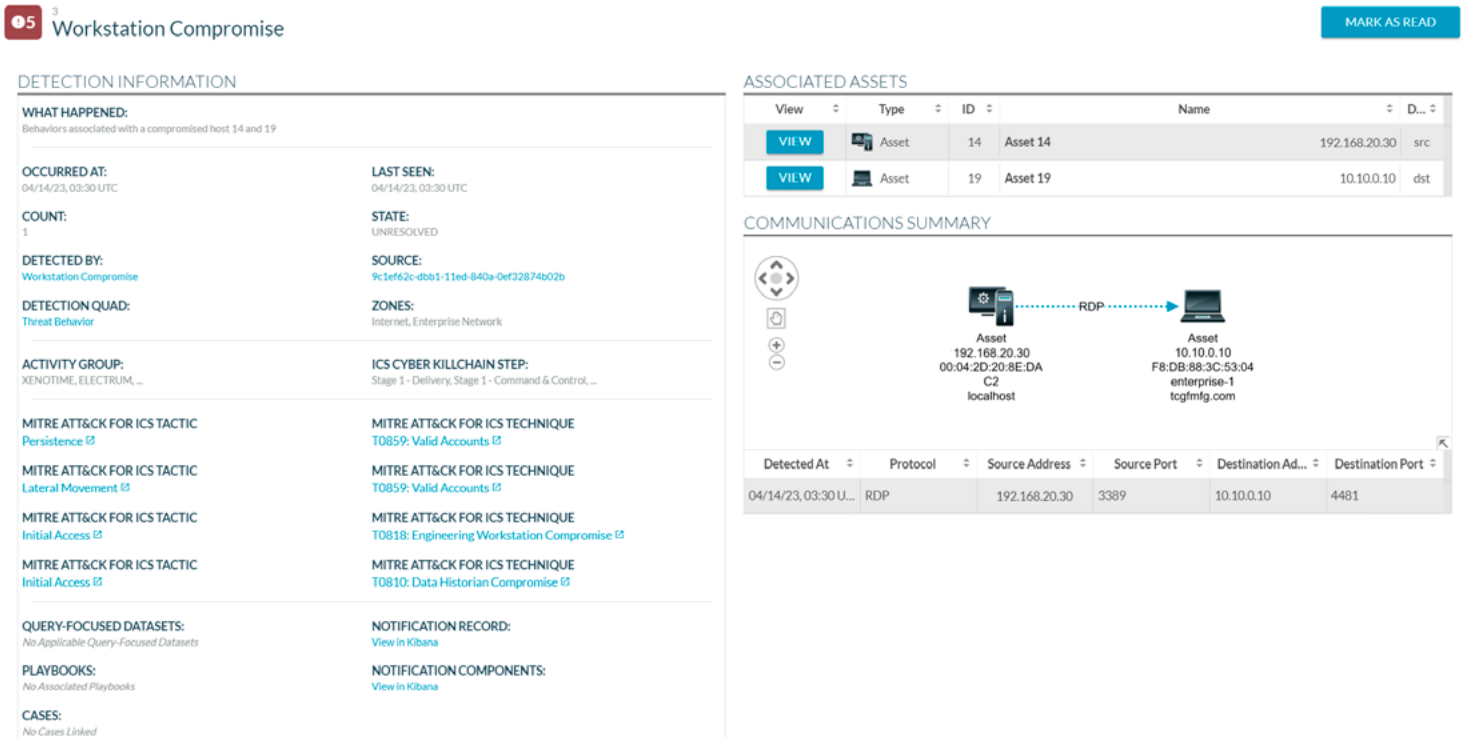


Diagram 5: Workstation compromise alert from the Dragos Platform

Improved Asset Visibility for Better Firewall Policy

The compromised asset in the DMZ communicating for the first time with another asset located in the OT environment using RDP, detected by the Dragos Platform. The Dragos Platform also detects multiple login attempts, and in a time frame where administrate traffic is usually not present in the network. The combination of all these characteristics triggers an alert about a possible workstation compromise. The asset is automatically assigned to an address group, set by the Palo Alto Networks Next-generation firewall for further investigation and/or actions as per security policy.

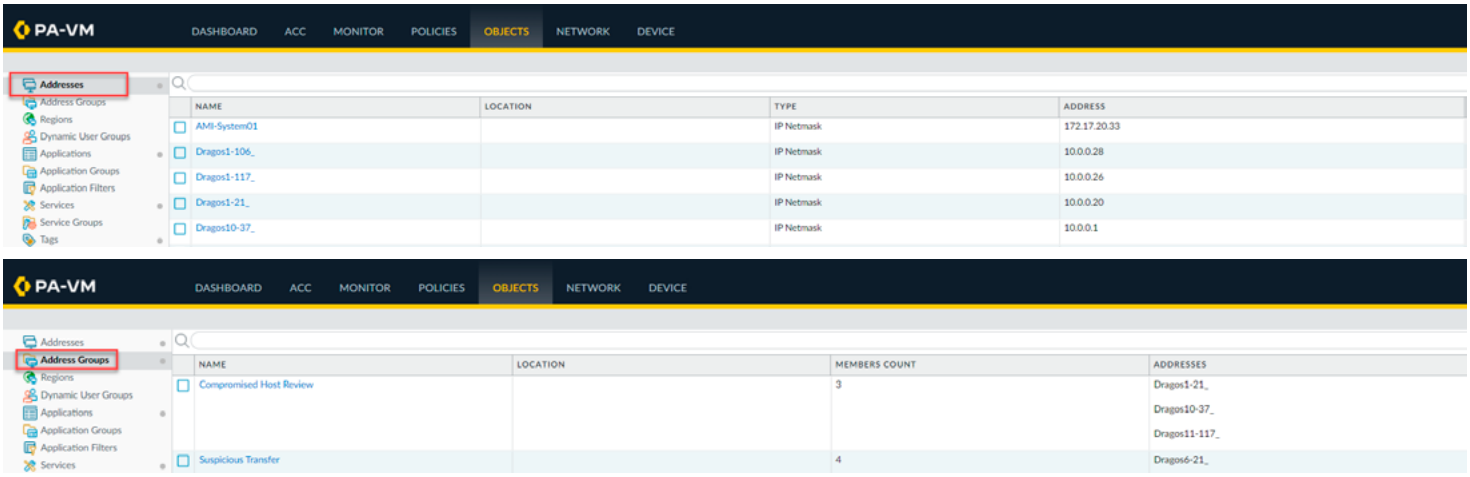


Diagram 6: Address and Address Group in Palo Alto Networks Next-Generation Firewall

Enhanced IT/OT Network Perimeter

This quickly prioritizes, investigates, responds to threats and provides network segmentation to reduce threats from moving unchallenged laterally through the network. This action saves the OT assets from the intrusion or tampering that a successful IT attack might have tried. This also stops the attack early in the process and prevents it from spiraling into a major incident that could potentially affect both IT and OT operations. Without network visibility or enforcement of security policies with a firewall, there is nothing stopping attackers from manipulating the control systems, disrupting processes, or stealing sensitive information.

Learn More

This white paper is based on a recent webinar, **Implementing A Defensible Architecture in the Power Industry: How Palo Alto Networks and Dragos Empower Your ICS/OT Cyber Security Journey**, presented by Dragos Senior Industrial Consultant Jose Avila-Gomez, Dragos Chief of Staff Phil Tonkin, and Palo Alto Networks ICS and SCADA Systems Expert Security Architect, Lionel Jacobs.

For more information on the Palo Alto Networks partnership, please visit: www.dragos.com/partner/palo-alto-networks/

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us