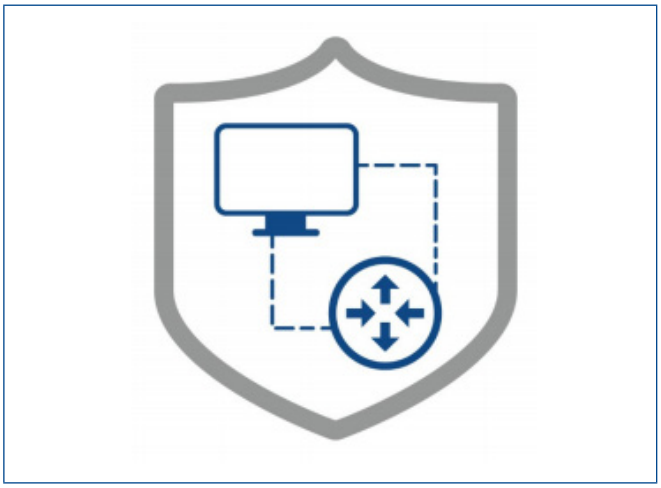
Threat Monitoring Solutions for DeltaV™ Systems

- Identify system assets
- Visualize network communication
- Detect network anomalies and risks
- Respond quickly to potential threats



Introduction

The cybersecurity landscape is constantly changing. New threats and vulnerabilities that directly impact both operational technology (OT) and information technology (IT) are regularly emerging at an increasing rate. At the same time, maintaining secure systems, keeping up with product lifecycles, and ensuring systemwide compatibility are complex challenges. At Emerson, our goal is to simplify cybersecurity by streamlining threat intelligence, reducing investments in maintenance and lifecycle planning, and customizing solutions that meet unique customer goals.

Emerson's Threat Monitoring Solutions for DeltaV™ Systems are the latest evolution in helping customers identify cyber-threats that may impact operations, while proactively improving a system's cybersecurity posture. The Threat Monitoring Solutions for DeltaV Systems augment the existing defense-in-depth strategy that help safeguard people, assets, and data from cyber-threats. Incorporating data collected by Threat Monitoring Solutions from DeltaV Systems adds an additional layer of protection that complements Emerson's robust portfolio of security offerings for industrial control systems.

Threat monitoring is a flexible solution that can be deployed in a variety of configurations. Once deployed, the solution passively monitors and decodes network traffic to gain a detailed understanding of all traffic happening across a system. This results in access to robust system data that is parsed by intelligence driven analytics and presented to the user in a prioritized and usable manner.

Passive data collection means that no agents or active queries are directed towards the DeltaV system. DeltaV Smart Switches run mirroring code that is set to not impact DeltaV system control communications. This approach enables DeltaV system users to enjoy cybersecurity data visibility without compromising the industrial control system's performance.

EMERSON™

Benefits

Identify System Assets: A result of passively monitoring mirrored traffic on the area control network is that the Threat Monitoring Solutions can identify all system assets (even when unauthorized components are connected to the wrong networks). The manual and error prone tasks of keeping asset inventories, walking down plants, and determining the proper reoccurring maintenance cycle, are replaced by a simple, near real-time solution that reduces costs, eliminates errors, and minimizes the need to schedule manual asset inventory updates.

Visualize Network Communication: Threat Monitoring Solutions track information being shared and how data is moving across a network. This provides system owners with a clear understanding of how their networks are segmented and visibility into how network controls are managing system data. Visibility of network communications happens in a list as well as graphical/visual format to facilitate decision making.

Detect Network Anomalies and Risks: During commissioning of the Threat Monitoring Solution, the control system baseline of communications is defined so that anomalies can be more easily identified. A core benefit of Threat Monitoring Solutions is to detect malicious and/or irregular traffic. By watching the network traffic within or across networks, these solutions will quickly discover and prioritize threats and potential vulnerabilities through intelligence-driven analytics. Extensive protocol libraries allow Threat Monitoring Solutions to work seamlessly in various configurations and evaluate DeltaV system network traffic.

Respond Quickly to Potential Threats: Threat Monitoring Solutions augment the process of performing incident response for DeltaV systems. Threat Monitoring Solutions require ongoing utilization since it is a continuous process of analyzing data and outcomes generated by the solution platforms. One of the key advantages to Threat Monitoring Solutions is the ability to prioritize events so that users can make informed and timely decisions.

Strategic Agreements

Aligning market demand with best-of-breed solution providers allows Emerson to focus on key agreements to enable Threat Monitoring Solutions for DeltaV Systems. DeltaV system network monitoring has been available for DeltaV systems for some time, so adapting the system architecture to include Threat Monitoring Solutions is simple and requires no changes to the DeltaV system network since the data collection is done passively. The agreements with Dragos and Nozomi Networks strengthen Emerson's OT cybersecurity expertise and services with proven solutions for control system environments.

The Dragos platform offers flexible deployment options. It includes one or more sensors that are strategically placed within a DeltaV system network. Aggregation switches can be used to combine traffic from multiple control network sources before being connected to a Dragos sensor. The Dragos sensor(s) then connect to a central Dragos SiteStore to allow for central management, visibility, and reporting. Once installed, the Dragos platform can be used as a standalone system or integrated into Dragos OT Watch, Neighborhood Keeper, or other solutions that tap into Dragos's experienced team of ICS/OT experts.

Nozomi Networks unlocks asset visibility and threat detection by flexibly deploying remote collectors and sensors within a DeltaV network. Aggregation switches can also be used to monitor traffic from multiple control network sources for cyber-threats and network anomalies. Visibility is available via the sensors' web interface, or through the optional Central Management Console when integration of multiple sensors into a single dashboard is required. Nozomi's solution can be enhanced with additional components: Smart Polling, Threat Intelligence and Asset Intelligence which can all be provided as a subscription service. The Nozomi Networks platform can also be managed in a SaaS model through its Vantage offering.

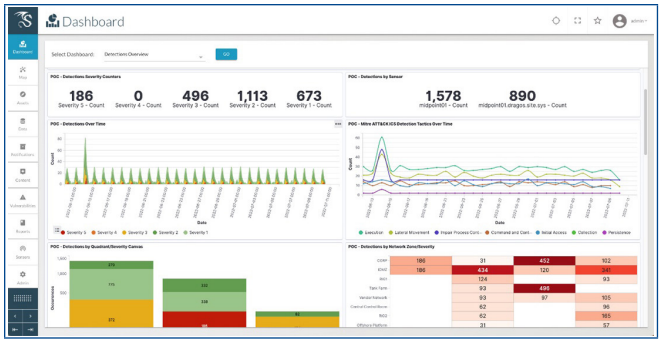


Figure 1: *Example Dragos Dashboard.*

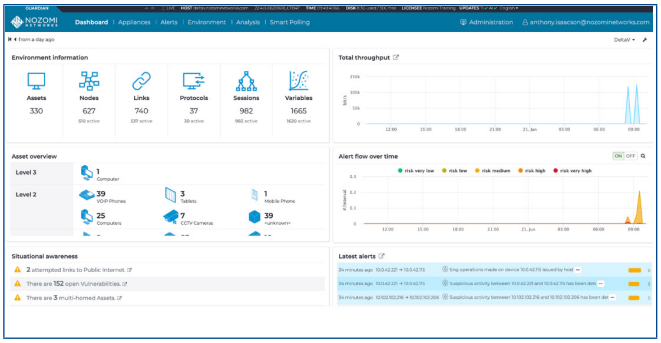


Figure 2: *Example Nozomi Dashboard.*

Threat Monitoring Solution Reference Architecture

The below diagram shows an example deployment of a Threat Monitoring Solution. Both Dragos and Nozomi have different naming conventions for their respective devices, so to simplify, a common naming convention is used in the diagram below. While each unique Dragos or Nozomi installation can differ, both will deploy at least one sensor or collector, which is identified on the diagram as a Threat Monitoring Sensor.

The Threat Monitoring Sensor is connected to a DeltaV Smart Switch (or Switches) where desired traffic is to be monitored. Each DeltaV Smart Switch that is to be monitored will need to be configured for port mirroring. In the diagram below, an optional Central Monitoring Switch has been added, which allows for data aggregation. This provides expansion capabilities, so that many switches can be connected to one Threat Monitoring Sensor.

In most cases, the Threat Monitoring Sensor will tie back to a Threat Monitoring Dashboard, as is depicted in the diagram. For Dragos this is the SiteStore and for Nozomi Networks this is the Central Management Console. The Threat Monitoring Dashboard acts as the User Interface, while also being able to perform management functions for the solution. The Threat Monitoring Dashboard can be connected to multiple Threat Monitoring Sensors, which allows for a centralized solution that can be deployed across many DeltaV systems.

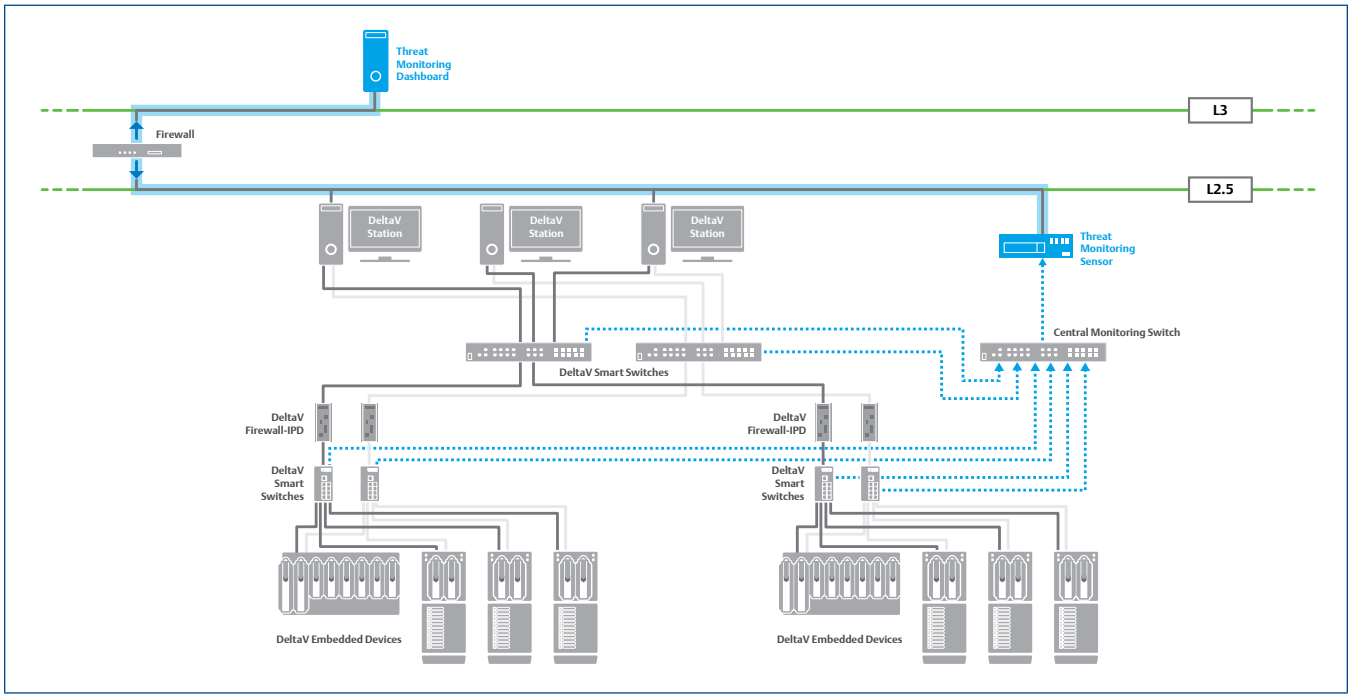


Figure 3: *General Architecture for Threat Monitoring Solution.*

Service Description

Architectural Consultation: Because each system is unique and requirements can vary, the service begins with a network architecture consultation to ensure the best overall deployment for your organization. Emerson best practices and knowledge of DeltaV systems ensure the selected Threat Monitoring Solution is able to capture critical network traffic.

Installation Services: On-site installation services are provided to validate the Threat Monitoring Solution is properly configured to collect critical traffic across the DeltaV network. It is recommended that this service is performed during non-critical plant operation; however, it is possible to install the Threat Monitoring Solution while a system is online if required.

Customization: Emerson's certified specialists can optionally assist with customizing dashboards, configurations, alerting, and visualization depending on your security policies, compliance requirements, or operational preferences.

Training Services: Threat Monitoring Solutions for DeltaV systems allow you to have unparalleled visibility into the network security of the DeltaV control system. Emerson certified specialists can train your local engineer or IT personnel to understand how the solution works and maximize its benefits.

Tuning Services (Operationalization): Within a couple of weeks of commissioning, the Threat Monitoring Solution will reach its optimum state of asset identification and normalization of network flows (baseline). Emerson offers an optional service to help users fine-tune the Threat Monitoring Solution implementation while unveiling to the user all the benefits of the solution. This service can be done remotely, but it is more comprehensive if done at the site where the solution has already been implemented.

Maintenance Services: Systems change over time; firewall rules are modified, assets are added, removed, and replaced, and technology evolves. Maintenance visits are typically purchased in a bank of service hours to routinely ensure that the Threat Monitoring Solutions are tuned properly to interface with the current state of your DeltaV system.

Post-Project Support Services: Threat Monitoring Solutions are not covered under Emerson's Guardian service contracts; therefore, Emerson will always include post-project support for any specific customer consultation with regards to project deliverables.

Configuration Updates: Threat Monitoring Solutions rely on regular content updates to identify new protocols or previously unknown threats. The annual support subscription ensures that the latest content updates are available to your system.

Incident Response: Emergency on-site services are also available separately to provide expert investigation, forensic analysis, and consultation. Emerson experts can augment your incident response or provide end-to-end investigation.

System Compatibility

The deployment of Threat Monitoring Solutions for DeltaV Systems is compatible with the currently supported DeltaV releases. DeltaV Smart Switches need to be running up-to-date firmware to enable port mirroring functionality. DeltaV Safety Switches can be updated with firmware that has port mirroring enabled on demand.

Please review the white paper DeltaV Smart Switches Port Mirroring for more information.

Ordering Information

Emerson offers Threat Monitoring Solutions for DeltaV Systems as engineered solutions that are designed, implemented, and supported by certified professionals. For inquiries and ordering information, please contact your local Emerson sales office. Prior to order acceptance, Emerson will issue a written proposal for your review and approval to ensure that scope, deliverables, timing, and budget meets your needs and expectations. Emerson support for Threat Monitoring Solutions is only offered to installs and upgrades performed by Emerson certified professionals.

Related Products

Threat Monitoring Solutions is an advanced set of solutions that are part of the broader DeltaV cybersecurity portfolio. Consider adding the following cybersecurity solutions and services to get the best protection for your DeltaV systems:

- Endpoint Security for DeltaV Systems
- Application Whitelisting for DeltaV Systems
- Emerson NextGen Smart Firewall
- DeltaV Firewall-IPD
- DeltaV Smart Switches
- Security Information and Event Management (SIEM) for DeltaV Systems
- Backup & Recovery
- Integrated Patch Management for DeltaV Systems

To learn more about how Emerson's comprehensive Cybersecurity Management Services can address your cybersecurity needs, contact your local Emerson sales office, or visit **www.emerson.com/deltavcybersecurity**.

Contact Us
www.emerson.com/contactus

EMERSON™