# Security Information and Event Management (SIEM) for DeltaV™ Systems

- Integrate security operations
- Achieve security intelligence
- Enable rapid threat response
- Deliver compliance results

*Establish an active defense posture with real-time situation awareness of cybersecurity on the DeltaV™ network.*

## Introduction

Enterprise IT organizations are routinely requesting a view into the security of control systems. However, IT personnel rarely have direct access to the control system layer. With Security Information and Event Management (SIEM) for DeltaV™ distributed control system (DCS), complete and correlated access to the content and context of security events in the control system layer is now possible for IT.

The SIEM for DeltaV Systems can be specially tailored to provide security logs, events, and information to improve your organization's security intelligence and situational awareness. With real-time analysis and alerts, your security team can proactively respond to events.

SIEM for DeltaV Systems is available as a virtualized solution designed to reside in your network's DMZ layer. The Emerson Smart Firewall ensures the data is securely transferred from the control system layer.

Events and logs contain a wealth of information that is rarely consumed. Imagine the manpower required to sort through Windows and system events and logs one-by-one. The SIEM for DeltaV Systems can be set up to allow you to proactively monitor security events and logs in real-time by correlating information and event logs from your integrated DeltaV control system, including:

- Windows Events and Syslog
- Network Device

Emerson's service specialists can help you deploy the SIEM for DeltaV Systems by providing the following services:

- Architectural Consultation
- Installation Services
- Training Services
- Maintenance Services
- Configuration Updates
- Incident Response

## Benefits

**Integrate security operations:** Provide your IT organization with the security information to perform advanced threat detection for your critical infrastructure. Emerson's SIEM solution can seamlessly integrate with your enterprise IT operations, such as a centralized Security Operations Center (SOC). Logs and events can be provided in the format that IT organizations need.

*Logs and events can be displayed in user-friendly dashboards to provide actionable intelligence.*

**Achieve security intelligence:** The SIEM for DeltaV Systems can be tailored to deliver the most relevant security information from the DeltaV control system. Emerson's available comprehensive set of rules, alerts and user-friendly dashboards can be applied to discover security use-cases specific to DeltaV Systems.

**Enable rapid threat response:** Data can be collected and analyzed in real-time to provide prioritized alerts, enabling you to discover and thwart potential threats as they are occurring. Shift your defensive posture from passive to active with actionable intelligence, which enables you to identify, understand and respond to cyber threats.

**Deliver compliance results:** Events and information can be stored in the optional historical database for queries, forensics, rules validation and compliance reporting. Historical data empowers you to analyze patterns and perform anomaly detection once your baseline is established.

## Service Description

**Architectural consultation:** Because every customer has their own network architecture, the service begins with a network architecture consultation to ensure the best overall deployment for your organization. Emerson best practices ensure your network is both secure and compatible with the SIEM for DeltaV Systems.

**Installation services:** On-site installation service is available to ensure the appliance is configured properly to collect security information and events from all DeltaV nodes and network devices. Installation can be performed without a reboot of your DeltaV nodes.

**Customization:** Emerson's certified specialists can optionally assist with customizing rules, alerts, dashboards, and automated report generation depending on your security policies and compliance requirements.

**Training services:** SIEM for DeltaV Systems puts you in the driver seat to monitor the security of the DeltaV control system layer. Emerson certified specialists can train your local engineer or IT personnel to monitor the appliance and understand the alerts.

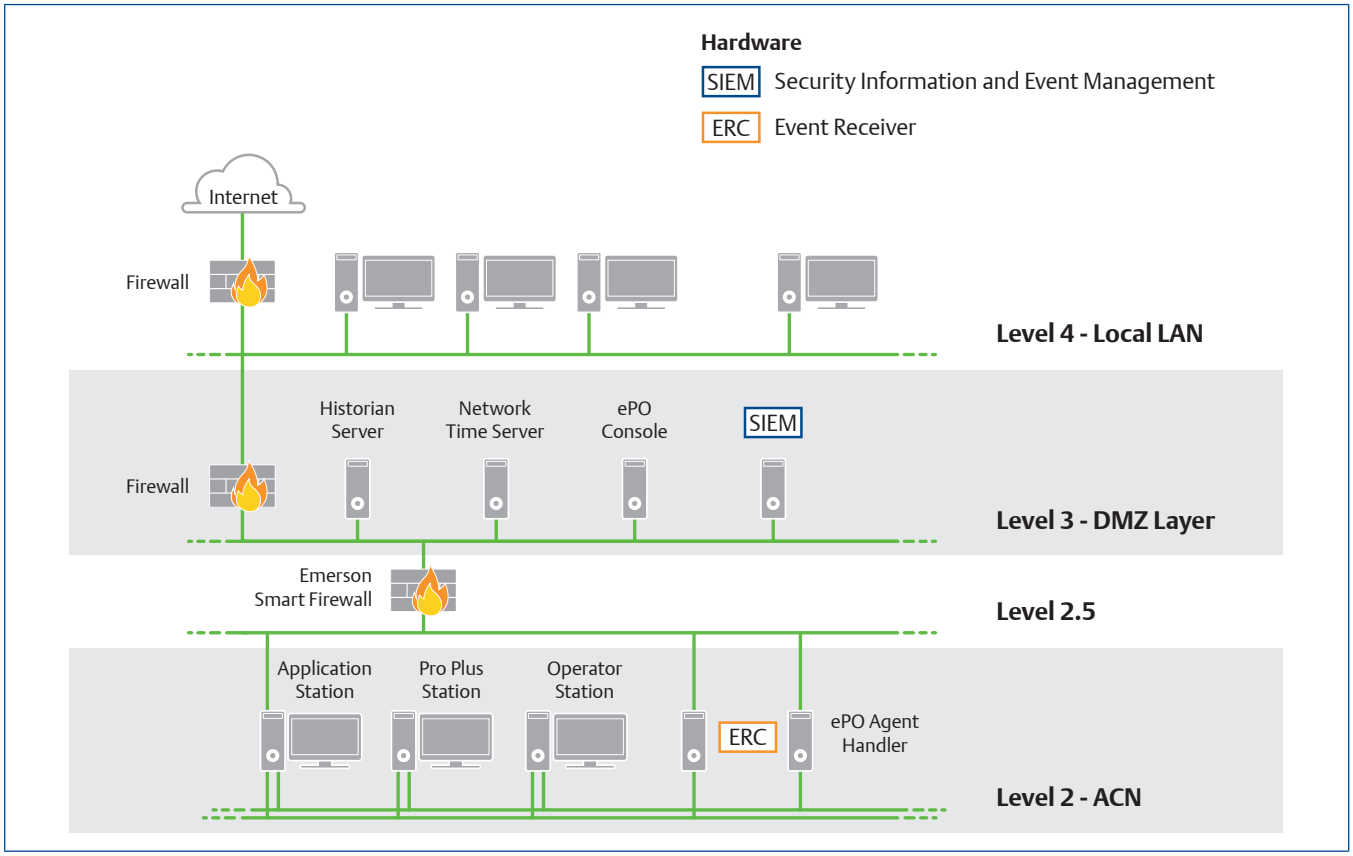
**Maintenance services:** Maintenance visits are typically purchased in a bank of service hours to routinely check the historical logs and communication integrity with your DeltaV nodes. Certified engineers can also investigate anomalies and help identify potentially malicious activity.

**Configuration updates:** Emerson will update the configurations, dashboards and rules as needed to improve security visibility of your DeltaV System assets. The annual support subscription ensures that you will have access to the latest updates. Emerson SME support and call escalation to Trellix are also included.

**Incident response:** Emergency on-site services are also available to provide expert investigation and forensic analysis.

## System Compatibility

The deployment of SIEM for DeltaV Systems software is compatible with the currently supported DeltaV releases. Please consult the Complementary Products List for full details. A Network Time Protocol (NTP) Server is required to synchronize time between the DeltaV System and the SIEM. A downstream (Level 2) server, such as a DeltaV Application Station, will host the necessary syslog software to gather network device logs and forward them to the SIEM. Likewise, a downstream non-DeltaV server will host a software agent to forward Windows events to the SIEM. It is recommended to use the Emerson Smart Firewall in order to forward the events and logs in a secure manner.




*Example reference architecture for SIEM for DeltaV Systems on a typical DeltaV network.*

## Virtualized Option

The virtualized SIEM for DeltaV Systems can be installed on either VMWare ESXi or Hyper-V host. The virtual machine is available in two classes, depending on the size of your DeltaV System:

- SIEM50 – for use with small DeltaV systems or sending parsed logs and events up to Security Operations Centers off-site. Limited to 500 Events per Second and maximum of 50 data sources.
- SIEM100 – for use with most larger DeltaV Systems. Please note: If the customer requires a physical SIEM appliance, then this must be ordered from Trellix as a direct buy-out. The physical appliance subscription support part number VE9128GxMD-S must be ordered and maintained annually for Emerson support.

## Ordering Information

| Description | Model Number |
|---|---|
| Security Information and Event Management (SIEM) for DeltaV Systems | Please Contact Your Local Emerson Sales Office |
| One Year Warranty and Support for SIEM for DeltaV Systems | Please Contact Your Local Emerson Sales Office |
| Installation Services | Please Contact Your Local Emerson Sales Office |

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 meet your needs and expectations. Standard solution support is only offered to installs and upgrades currently performed by Emerson certified SIEM professionals.

## Related Products

SIEM for DeltaV Systems is part of Emerson's suite of Trellix Solutions for DeltaV Systems. Consider the following complementary products to get the most out of your SIEM for DeltaV Systems:

- Endpoint Security for DeltaV Systems
- Application Whitelisting for DeltaV Systems
- Network Security Monitor for DeltaV Systems

To learn how comprehensive Cybersecurity Management Services address your cybersecurity needs, contact your local Emerson sales office or representative, or visit **www.emerson.com/cybersecurity**.

***Legal Disclaimer:***

*This product and/or service is expected to provide an additional layer of protection to your DeltaV system to help avoid certain types of undesired actions. This product and/or service represents only one portion of an overall DeltaV system security solution. Emerson does not warrant that the product and/or service or the use of the product and/or service protects the DeltaV system from cyber-attacks, intrusion attempts, unauthorized access, or other malicious activity ("Cyber Attacks"). Emerson shall not be liable for damages, non-performance, or delay caused by Cyber Attack. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the security products.*



**Contact Us**
**www.emerson.com/contactus**

DeltaV™

EMERSON™