

Event Manager

TURN CYBERSECURITY DATA INTO INSIGHT IN REAL-TIME

Security analysts have massive quantities of data at their disposal. And somewhere in that accumulation of data are security events that require quick action to stop an attack or prevent a breach. But those important security events are mixed in with events that require no action at all.

Reviewing, analyzing, and prioritizing large volumes of security data is inefficient and susceptible to human error—especially when the data is presented in different formats your analysts are unfamiliar with.

[Event Manager](#) is a cybersecurity insight and response platform that ensures critical events get the attention they require.

Events are translated into an easy-to-interpret format, and critical events are separated from the noise in real time. This enables security analysts to act quickly and decisively, even without specialized knowledge of every technology in your environment. A full audit trail makes it easy to meet compliance requirements.

INTEGRATE SECURITY EVENTS FROM ACROSS YOUR ENVIRONMENT

Every organization is unique and requires a different set of tools in order to run smoothly. With out-of-the-box templates for integrating numerous assets like Windows servers, Oracle databases, or Cisco networking devices, it's simple to get started on streamlining your data quickly. Event Manager also leaves no device behind, providing a tool for converting custom data sources so they are also fully integrated.

TRANSLATE SECURITY EVENTS INTO A COMMON FORMAT

Event Manager collects security events from sources across your environment, no matter how the events are formatted. These disparate events are translated into a single format that's easy for security analysts to understand.

Using a common format saves time. Analysts are able to work faster when they're not forced to interpret information presented in multiple formats. Event Manager also eliminates the need for on-staff expertise related to the different sources of security events.

PRODUCT SUMMARY

KEY FEATURES

- Real-time identification of internal and external threats
- Easy-to-interpret common format for security events
- Prioritization of serious issues for a rapid response
- Proactive security monitoring
- Greater visibility into security posture
- Custom report building for versatile analysis
- Scheduled reporting to ensure compliance
- Event correlation rules
- Complete audit trail
- Integration with third party applications

PLATFORMS MONITORED

- Operating Systems like Windows and Linux
- Cloud (Public, Private, Hybrid)
- Databases
- Web Services
- Network Appliances
- Software Applications
- Your Custom Critical Data

SYSTEM REQUIREMENTS

- Windows Server 2012 or higher
- SQL Server 2012 or higher

SEPARATE CRITICAL EVENTS FROM THE NOISE

When every security event carries equal weight, it's easy for analysts to miss important information and potentially leave your organization vulnerable to sophisticated cyberattacks. Event Manager escalates the criticality of serious issues, reducing alert fatigue and ensuring analysts don't waste time and only focus on security events that require action or attention. In addition to default settings filtering out insignificant information or benign threats, users can fine tune the data they see, and add inclusion/exclusion rules about what exactly should be processed by Event Manager. Additionally, users can adjust within the dashboard itself, selecting and filtering out alerts that appear that they no longer want to view in the future.

CUSTOMIZED REPORTING TO SUIT YOUR ORGANIZATION'S NEEDS

Easily generate built-in reports designed to highlight compliance with regulations like PCI-DSS. Reports can be conveniently scheduled to generate at any time.

Additionally, create any report you need with an intuitive interface to highlight any events, threats, and incidents. Reports are fully searchable and can also be exported into a variety of formats (PDF, CSV, DOC, XLS).

COMPLETE AUDIT TRAIL

Event Manager documents the process of a security analyst's forensic investigation, including notes for closed cases and reported incidents. This makes it easy to meet common compliance mandates that require proof of regular security monitoring.

FREE VERSION

- Same core features of Event Manager
- Ideal for small to mid sized businesses

RELATED PRODUCTS

- [HelpSystems Insite](#)
- [Security Auditor](#)
- [Identity & Access Manager \(BoKS\)](#)
- [Interact](#)
- [Vityl](#)

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.