FORTRA™

DATASHEET (TRIPWIRE)

Enrich your SIEM with Compliance and Change Intelligence

Stay ahead of emerging threats with IBM Security and Tripwire

Cybercriminals are more sophisticated than ever, and the attacks on all types of organizations show no signs of slowing down. That's why IBM Security, Tripwire and a wide range of security industry leaders have joined forces on the IBM Security App Exchange—so security teams from around the world can work together to create better cyber defenses.

Reduce risk with Tripwire App for QRadar

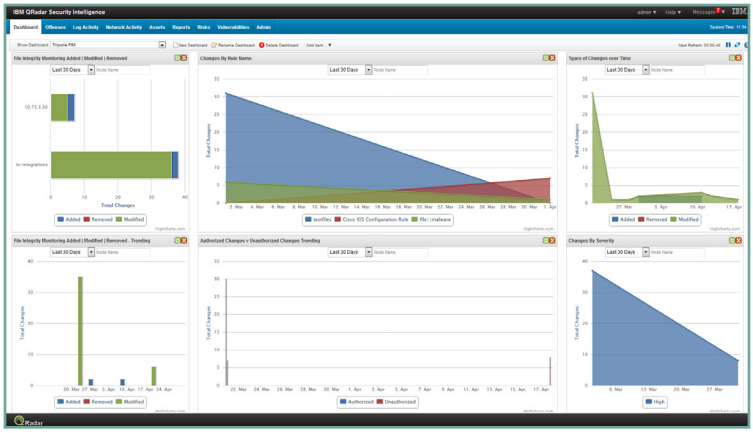
Using Fortra's Tripwire App for QRadar, you can incorporate file integrity monitoring and security configuration management data into IBM QRadar for reporting, forensics, and correlation. Reports and dashboards are provided for visualizing this intelligence within your own QRadar dashboards. Forensic capabilities include a right-click context menu item for IP addresses in QRadar to easily search Tripwire® Enterprise for relevant nodes with changes or failing compliance rules. Correlated data points like changes occurring after failed logons, or changes made by suspicious user during odd hours can quickly add color to an incident.

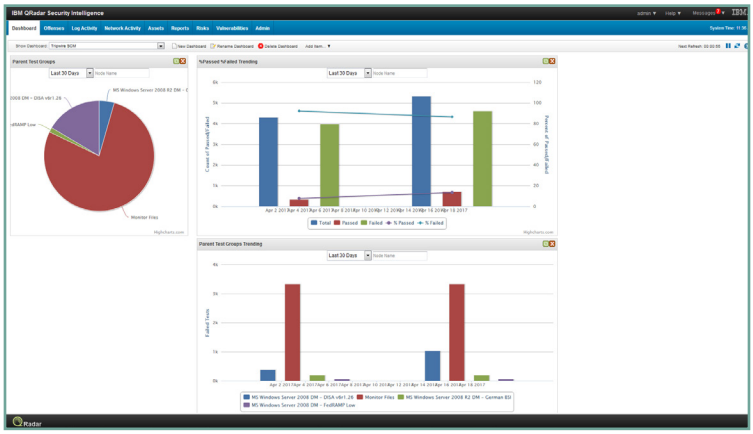
Additionally, real-time change detection in Tripwire Enterprise, triggered by events or rules in QRadar, reduces investigation costs and mean time to remediate incidents. For example, this solution includes out-of-the-box support for real-time checks of Cisco IOS devices that are sending syslog events in QRadar. When a user logon/logoff is detected for a device, a scan is triggered and results sent to QRadar.

IBM SECURITY

The IBM Security App Exchange provides organizations with:

- Convenient web access to validated extensions to IBM Security solutions
- Additional IBM® Security QRadar® correlation rules, dashboards, visualizations and third-party integrations
- The ability to share content with industry peers to help eliminate threats





Using the Tripwire App for QRadar, you can connect to a Tripwire Enterprise console and ingest FIM and SCM data into QRadar. Dashboard items are provided so that you can visualize this data within your own QRadar dashboards. Perform real-time checks against nodes in Tripwire Enterprise triggered off of IP addresses from any events by creating rules in QRadar.

Includes out-of-the-box support for real-time checks of Cisco IOS devices that are sending syslog events in QRadar. Includes a right-click context menu item for IP addresses in QRadar to easily search the Tripwire Enterprise console for relevant nodes.

FORTRA™
Fortra.com

About Fortra
Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

Business Partner IBM

IBM Security App Exchange
The IBM Security App Exchange is the premier collaboration site for sharing software enhancements, applications and extensions that complement IBM Security solutions. It enables security teams to access tools that help improve visibility into threats, anomalies and malicious activity occurring on the network. To learn more about the IBM Security App Exchange, please visit: apps.xforce.ibmcloud.com