Cisco ISE and Huntsman Analyst Portal

Benefits

- **Streamlines SOC operations** by automating workflows so that analysts can quickly focus on the real threats
- **Verifies decision making automatically** using information from both network and security devices
- **Defeats advanced attacks** by automatically quarantining them before they can affect the enterprise
- **Decreases time at risk to seconds** for high-confidence decision making and response

Cisco ISE and Huntsman Security integration

Automated threat verification for real-time response

In a world of too much data for too few analysts, enterprises are demanding faster and more accurate responses to security threats.

The Huntsman Analyst Portal®, now fully integrated with the Cisco® Identity Services Engine, empowers security operations center (SOC) teams to slash the time they need to investigate and respond to threats. The nature of a threat is automatically verified, dramatically reducing the time at risk from hours to seconds.

The system streamlines SOC workflows by compiling a casefile of all relevant threat information. This Automated Threat Verification (ATV) process determines the nature and severity of the threat in seconds.

False positives are eliminated, freeing up valuable time for analysts to focus on the threats that matter.

Analysts can manually investigate the Huntsman and ISE casefile before responding. Or, if appropriate, they can allow the process to proceed automatically with Cisco pxGrid for safe, simple, and rapid threat containment.

How the Solution Works

The Huntsman Analyst Portal® continuously monitors and correlates system activity from across the enterprise. It uses automation and machine learning to detect suspicious outliers or indicators of compromise.

By unifying Cisco ISE information with application, OS, user, and external information, the solution identifies any potentially malicious activity.

If any is detected, the ATV process is triggered to verify the nature and extent of the threat.

The portal quickly creates a casefile of all relevant threat information. Analysts can choose either to intervene in the decision-and-response process or permit the solution to proceed to an automated outcome.

One such automated action might be to quarantine an infected asset: safe and simple threat containment.

The Huntsman and Cisco ISE solution detects, analyzes, and responds to threats in real time—safe, automated actions that reduce the time at risk to deliver significant operational efficiencies and overall cost savings.

Next Steps

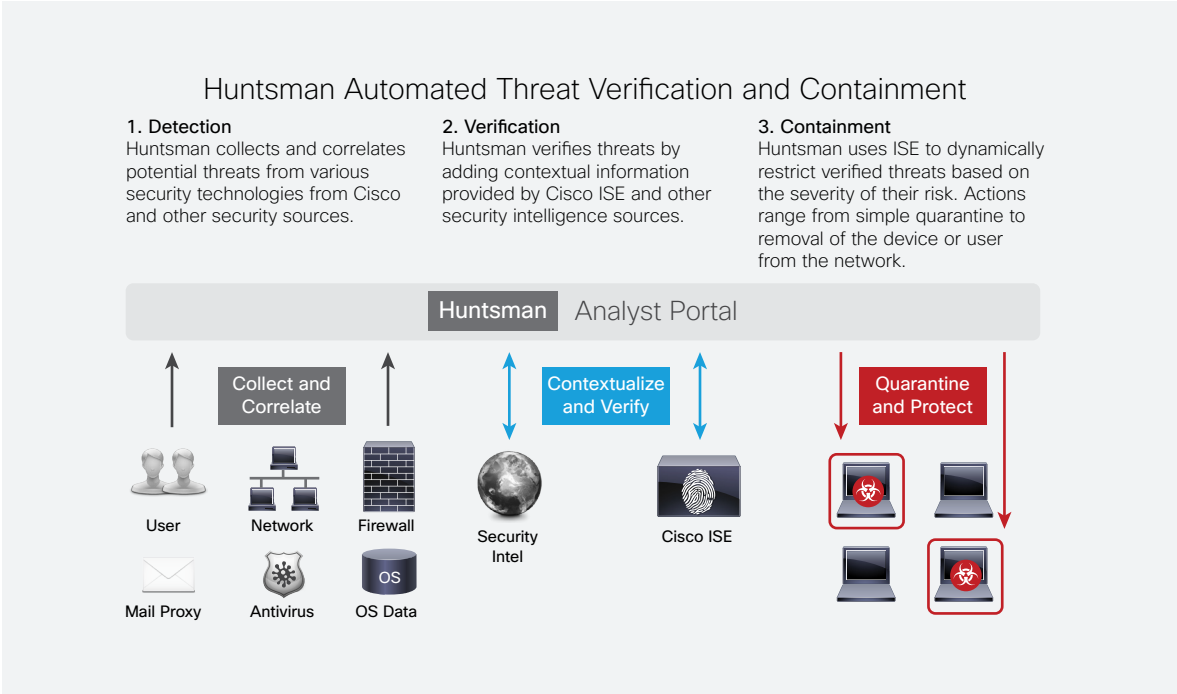
The integrated Cisco ISE and Huntsman Analyst Portal® security solution is in production in a number of critical SOC environments where its benefits have been proven. Learn how you can slash your time at risk, improve your security operations processes, and enjoy significant cost savings.

Request a demo: demorequest@huntsmansecurity.com

View the automation webinar, with detailed case studies (17 minutes)

"The increasing speed and accuracy of Security Analytics solutions is making it possible to automate security processes."

– Forrester Vendor Landscape: Security Analytics 2016.



C45-738690-00 03/17