Trellix

SOLUTION BRIEF

SOAR with Trellix Helix

Reduce security risk with security operations, automation, and reporting

Key benefits

- **Slash breach-response time.** Apply workflow automation, customizable dashboards, and pre-built playbooks that allow analysts to focus on high-priority tasks that reduce risk exposure.
- **Maximize the return on your existing security investments.** Take command of your security operations with hundreds of third-party plug-ins to firewalls, antivirus, and ticketing systems.
- **Reduce workload demands on analysts.** Implement customizable and fully automated workflows to reduce analysts' workloads and ensure process consistency.

Managing security operations is a challenge for any organization. Security teams employ many tools but still struggle to contend with increased alert volumes.

Unlike a traditional security information and event management (SIEM) that relies on manual intervention, Trellix Helix offers security orchestration that accelerates and simplifies your threat detection and response process by unifying disparate technologies and incident handling processes into a single console. With your security tools integrated, you can automate routine security tasks and focus on the threats that truly matter.

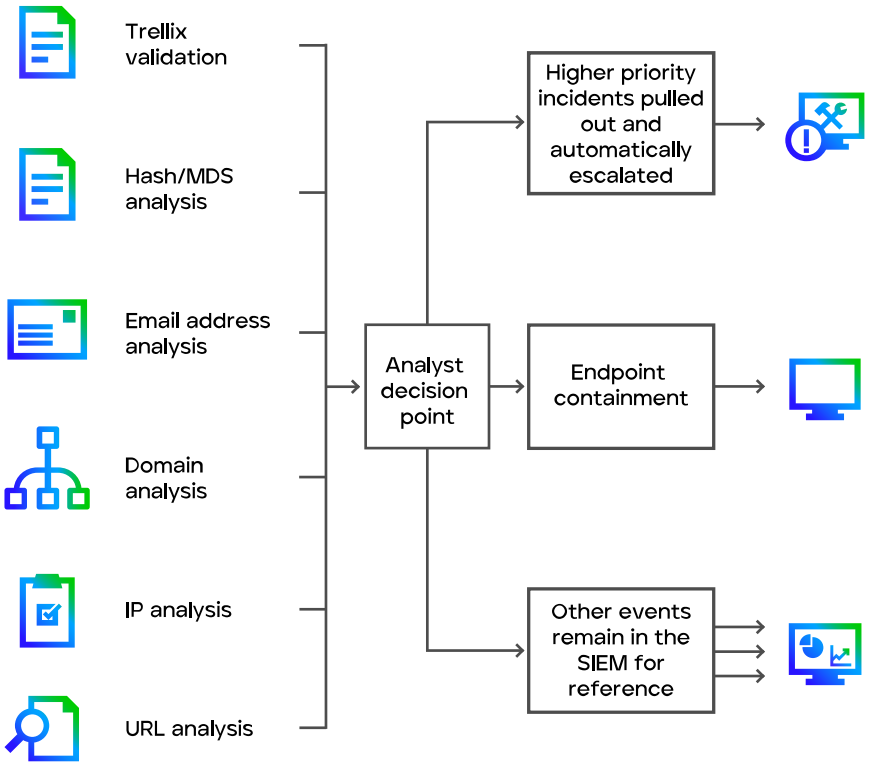

Figure 1. How Trellix security orchestration works

Additional capabilities

Incident response playbooks

Upskill your analysts and accelerate investigations with 400+ pre-built courses of action developed by Trellix incident responders. These may include assessment on image hashing and multidimensional scaling data analysis.

Open plug-in framework

Integrate more than 650 third-party tools and data sources for seamless, single-pane management of your security stack.

Process automation

Implement custom incident response workflow automation between your security appliances.

Case management

Enable collaboration between analyst and incident response teams by storing correlated alerts and artifacts in an intuitive case management system.

Case assignment

Create role-based groups and assign granular permissions playbooks for enhanced workflow management.

Intuitive user interface

Enable security teams to easily connect to security tools with a simplified abstraction layer to retrieve and push information. Manage changes at the network, host, and application levels.

How to get Helix

Helix is available standalone or with the purchase of Trellix's subscription-based solutions. It works across all Trellix technologies and helps integrate your installed base of non-Trellix security products. As your organization grows and changes, Trellix solutions can be reconfigured, added, or upgraded without disrupting organizational operations.

To learn more, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

Copyright © 2022 Musarubra US LLC 072022-01