SIEM Integration Module

Improve real-time visibility over managed and unmanaged devices while automating network access control and threat response

Highlights

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor managed devices, including corporate, BYOD and IoT endpoints

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints as determined by your SIEM product
- Improve compliance with industry mandates and regulations

Orchestrate

- Receive contextual information from your SIEM product and pro-actively take appropriate action
- Automate common workflows, IT tasks and security processes across systems
- Leverage the integration between ForeScout and your SIEM product to provide real-time view of threats across the enterprise

ForeScout Integration with SIEMs

ForeScout CounterACT is a network security appliance that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices and works with ForeScout ControlFabric™ Architecture to orchestrate information sharing and automate operation among disparate security and IT management tools.

The combination of using ForeScout CounterACT™ and a SIEM can result a significant increase in situational awareness and proactive risk reduction. Where most SIEM solutions offer situational awareness primarily through the collection of periodic log entries from many different products, they typically do not provide in-depth “real-time” endpoint data visibility. SIEMs are only as good as the information that is fed into them, and if the SIEM is not aware of all the network endpoints on a continuous basis, then it is not able to produce an accurate security snapshot of your network. This “gap” in endpoint visibility exists in SIEMs without CounterACT. CounterACT discovers network endpoints, and feeds that data into the SIEM, closing the endpoint visibility gap in your situational awareness.

By itself, a SIEM system doesn’t have any enforcement capabilities. Some SIEM systems are able to send commands to ForeScout CounterACT to automatically respond to endpoint security issues. For example: update the operating system, disable USB devices, or quarantine the endpoints.

The Challenges

Visibility. Any serious attempt to manage security risk must start with knowledge of who and what is on your network, including visibility to whether the devices on your network are compliant with your security standards. Most organizations are unaware of a significant percentage of the endpoints on their network because they are either not managed (BYOD, guest and IoT), have disabled or broken agents, or aren’t detected by periodic scans (transient devices). As such, you are unaware of the attack surface on these devices. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints connected to your network.

Threat Detection. Today’s cyber attacks are more sophisticated than ever. Multi-vectored, stealthy and targeted threats easily evade traditional security defenses such as firewalls, intrusion prevention systems, anti-virus platforms, and secure web and email gateways. Originating from highly motivated and well-funded threat actors and nation states, these attacks are focused on acquiring sensitive personal information, intellectual property or insider information. As the attackers have gained the upper hand, organizations are being compromised at an accelerating rate. In order to effectively detect and block these sophisticated threats, new security controls that do not rely on signatures are needed.

Response Automation. The velocity and evasiveness of today’s targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating a perfect storm for any incident response program. Without an automated system to monitor, install, update and reactivate security agents on managed systems, valuable time is lost performing these tasks manually. Without the ability to apply security controls to unmanaged endpoints (BYOD, guest and IoT), you are increasing your attack surface and putting your infrastructure at risk. And without a system to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyber threats to propagate within your network and exfiltrate data.

How it Works

When CounterACT discovers infected endpoints, it can receive instructions from the SIEM and automatically take policy-based mitigation actions to contain and respond to the threat. Various actions can be performed depending on the severity or priority of the threat, such as quarantine endpoints, initiate direct remediation, share real-time context with other incident response systems, initiate a scan by another third party product, or notify the end user via email or SMS.

1. Device connects to the network.
2. CounterACT informs SIEM system of device status.
3. CounterACT receives instruction from SIEM assessment of device based on events and logs collected.
4. CounterACT allows or denies access based on compliance assessment.

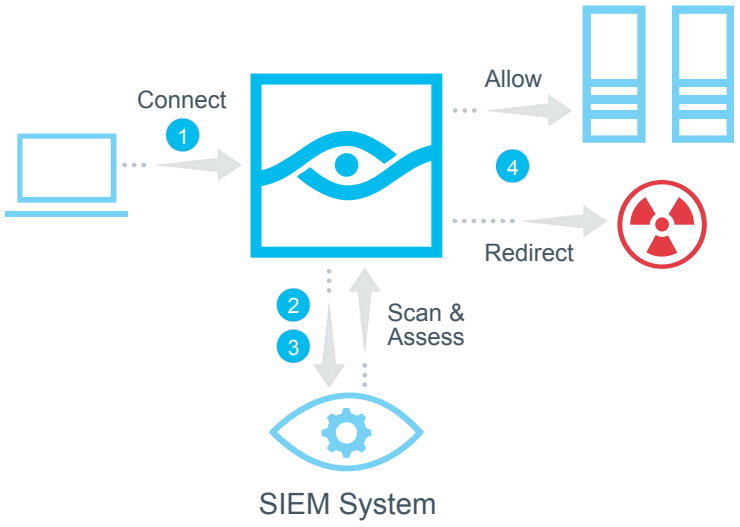

Figure 1: ForeScout CounterACT and your SIEM system work in concert to assess and manage devices as they access the network.

Supported SIEMs

SIEMs that are supported by the ForeScout SIEM Integration Modules are:

- ArcSight
- IBM QRadar
- Any SIEM that supports configurable messages in CEF, LEEF or plain Syslog

Note that different SIEM products have different capabilities in terms of correlating the data provided by CounterACT with data that it obtains from other sources. Also, SIEM products vary in their ability to send triggers to CounterACT; some SIEM products provide both manual and automated ways to trigger CounterACT to take action on an endpoint. For a more complete description of the features available with each specific SIEM product, talk with your SIEM vendor or read the joint solution briefs at www.forescout.com/solutions/siem.

For details on our licensing policy, see www.forescout.com/licensing.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284