White Paper

Cisco ISE Plus SIEM and Threat Defense: Strengthen Security with Context

What You Will Learn

Network security threats are a fact of life. But the modern security arsenal has two highly effective tools: security information and event management (SIEM) and threat defense (TD) solutions. SIEM and TD platforms can provide a wealth of information to help you quickly and accurately assess security threats and take immediate remediation actions, all from a single console.

Yet analytics are not enough. To build a proactive defense against even the nastiest threats, you need to integrate your SIEM or TD solution with the Cisco® Identity Services Engine (ISE).

Introduction

Nobody likes to think about it, but we all know they're out there: the bad guys, poking and prodding at your network, looking for an opening to get in and wreak havoc. And the ugly truth: As much money and brainpower as the industry is investing in security technologies, the bad guys continue to play offense, seeking to remain a step ahead.

SIEM and TD solutions provide crucial analytics to help you recognize when something suspicious is happening on your network. But valuable as these analytics are, they often lack relevant context, such as:

- Which specific user a threat is associated with
- What device is targeted
- What else is happening with that user and device that may be pertinent to understanding the severity of the potential threat

The real heavy lifting—translating an initial alert about a potential problem into an accurate assessment of the threat and identifying the specific user and device the threat is associated with—is still a time-consuming, largely manual effort. Mitigating that threat with a network action is even more challenging.

This effort is becoming exponentially more complicated with new IT trends. If assembling the relevant information to fully assess a threat is challenging in a traditional computing environment, the task is even more daunting in a world characterized by bring-your-own-device (BYOD) workplaces, software as a service (SaaS), and virtualization.

Or at least it was until recently. Now, next-generation network identity solutions such as Cisco ISE can integrate directly with market-leading SIEM and TD solutions. *Read more about ISE on page 6.*

SIEM and TD Tools: Made Even Better with the Right Context

To assess the appropriate role of SIEM and TD systems in your threat defense arsenal, it's important to understand what they bring to the table and how having the right context can increase their effectiveness.

SIEM and TD solutions provide vital information about what's happening in your network and help you spot anomalous activity that could represent a threat or compliance issue. This capability is an essential element in the security of your network. After all, the thorniest threats are the ones intelligent enough to hide themselves from standard network defenses. These “advanced persistent threats” may use a variety of routes and protocols to burrow into your network, look for opportunities to propagate themselves, and employ clever techniques to camouflage what they’re doing.

Modern SIEM and TD solutions comb through logs from a wide range of devices on your network to gather a holistic view of everything that’s happening and then analyze that data to flag suspicious or noncompliant behavior. These functions are extremely useful but do not always provide a complete solution. The result of all these analytics, after all, is a relatively broad identifying characteristic like an IP address. You need more information.

You don’t know who is associated with that IP address, you don’t know what they have access to, you don’t know which device is associated with that IP address, you don’t know whether that combination—user plus device plus level of access—represents a minor annoyance or a significant threat. To make that determination, you’re going to have to do more work, a lot more work, often manually pulling information from several monitoring and management consoles, before you can accurately assess the threat, much less take action against it.

Combining SIEM and TD with Contextual Identity and Policy Enforcement

Identity and policy-enforcement solutions such as Cisco ISE can provide the missing pieces to the threat defense puzzle and turn your SIEM or TD platform from a useful resource into a finely honed weapon against network threats.

Cisco ISE does this by bringing several important features to the table. The first and most important: user and device context.

Context

Instead of your SIEM or TD solution giving you just an IP address, for example, it can give you fine-grained detail on the source of that suspicious activity. This data includes:

- User information (name, authentication status, location, authorization group, quarantine status, etc.)
- Device information (manufacturer, model, OS version, MAC address, network connection method, location)
- Posture information (device compliance with corporate security policy, antivirus version, OS patches, compliance with mobile device management policy)

Armed with this information, you can quickly and accurately assess the significance of any security event. You can answer the critical questions:

- Who is associated with this event?
- Is it an important user with access to intellectual property or sensitive information?
- Is the user authorized to access that resource?
- Does the user have access to other sensitive resources?
- What kind of device is being used?
- Does this event represent a potential compliance issue?

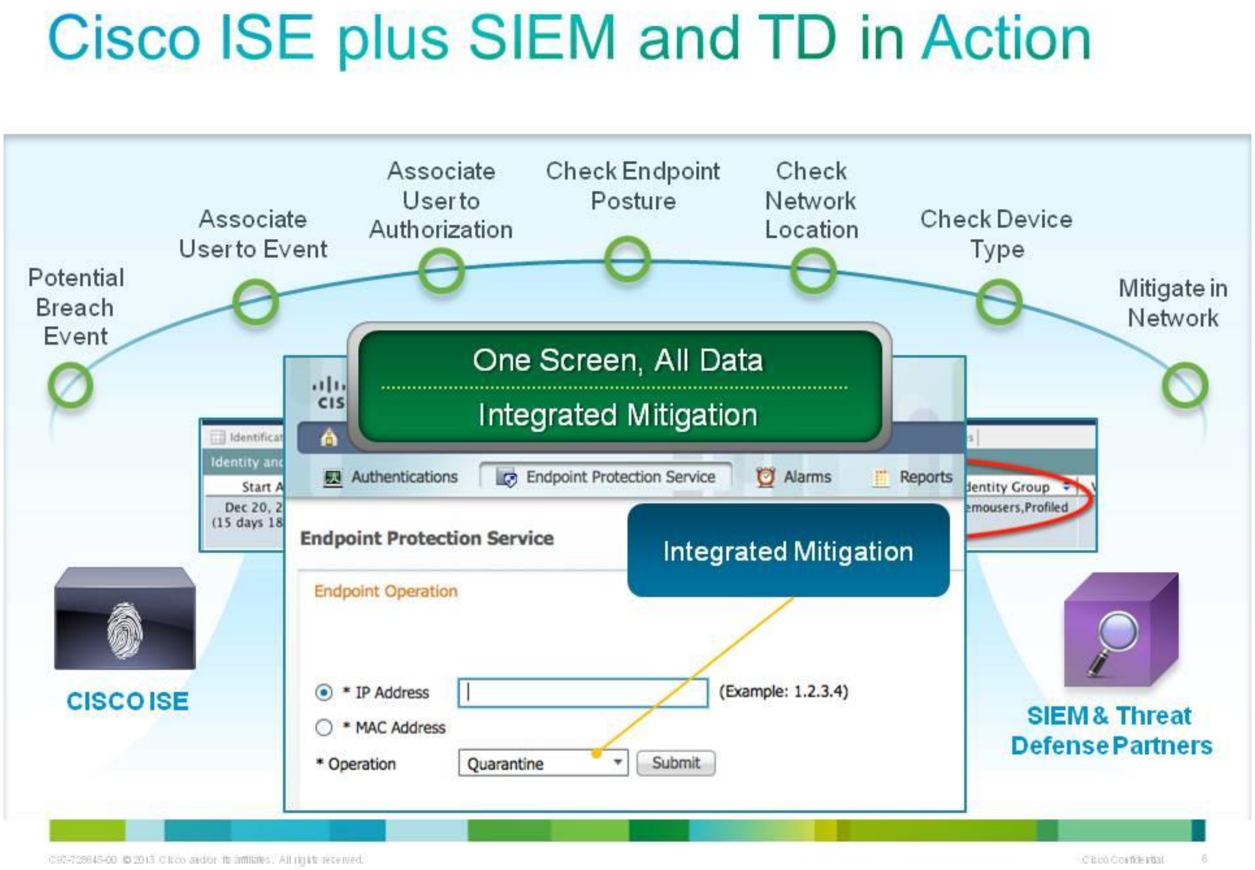
And you can answer these questions without ever leaving the SIEM or TD console.

Mitigation

The other essential element that Cisco ISE brings to the table is mitigation capabilities, integrated once again directly with the SIEM or TD platform (Figure 1). Cisco ISE provides more than just identity details; it uniquely and efficiently communicates with the network infrastructure to serve as the central point of policy enforcement for the network. Mitigation can take the form of Cisco ISE invoking a user or device quarantine policy, or a very precise mitigation action using Cisco TrustSec® network segmentation policies. *Read more about TrustSec on page 6.*

When you integrate these capabilities with your SIEM or TD platform, you can not only accurately evaluate the threat from within your SIEM or TD console, but also take action on that information immediately—quarantining a user or device, or even kicking it off the network entirely—from the same screen.

Figure 1 Cisco ISE with SIEM and TD Integration in Action



Endpoint Protection Service

Endpoint Operation

● * IP Address (Example: 1.2.3.4)

○ * MAC Address

* Operation Quarantine Submit

Advanced Security Monitoring

New capabilities derived from combining SIEM and TD systems with contextual identity and enforcement provide an invaluable tool to accelerate your detection of and response to security events. But these capabilities can also play an important role in helping you proactively manage security and compliance in today's more complex and dynamic network environments.

Cisco ISE provides your SIEM or TD solution with the additional context it needs, beyond standard links to Active Directory or the Lightweight Directory Access Protocol, to get real-time information about the user, device type, and security posture associated with any IP address. Regardless of whether the device is wired, wireless, associated with a human user, or just a machine like a printer, Cisco ISE tracks each device in real time. It captures the contextual information you need—device type, MAC address, authorization group, network location, etc.—to accurately evaluate it from a security or compliance perspective at any moment.

By connecting these dots, you can:

- **Provide a highly secure BYOD environment with device-driven security analytics:** With device profiling information coming from Cisco ISE, your SIEM or TD solution can build analytic policies based on the type of device that a potential security threat is associated with. For example, mobile devices may be considered a higher risk than IT-owned and IT-managed laptops. Using device-type awareness, SIEM and TD analytics can be configured to assign higher severity to events associated with mobile devices.

- **Perform identity- and authorization-driven security analytics:** Just as you can build analytics based on device type, you can also create analytics driven by the type of user, based on contextual information delivered by Cisco ISE to the SIEM or TD platform. For example, policies for guest users may have lower alert thresholds for certain types of events. You can also escalate the severity of suspicious events associated with IT administrators, who present a more significant risk given their level of access to critical systems. You can also closely scrutinize user groups with access to critical information.
- **Scrutinize devices with security posture failures:** If an endpoint has a posture failure and is generating suspicious security events, that endpoint is inherently more suspect than devices that have passed a posture check. Cisco ISE posture data used by SIEM and TD platforms can connect these dots without human intervention.
- **Generate reports on users, user groups, and devices:** Having a list of IP addresses for a policy or regulatory compliance audit is a good start. Having that information automatically associated with users, user roles, and device types makes reporting easier, more useful, and more convincing.

Benefits of SIEM and TD plus Superior Context and Mitigation

What do these new capabilities potentially mean for your business? They can help you:

- **Decrease time to security event classification:** The SIEM and TD platform can use Cisco ISE user, device-type, access-level, and posture information to answer common questions needed to make sense of a security event. It helps you find fast answers to questions such as: What user and device are associated with this event? What is the state of that device, and what does the user have access to? This context expedites the classification of security events, helping prioritize which events require further action.
- **Simplify compliance:** Drawing on the combined capabilities of Cisco ISE and your SIEM or TD platform, you can enforce a fine-grained security policy to meet diverse compliance requirements and quickly demonstrate compliance in internal and external audits.
- **Accelerate threat response times:** In most contemporary network environments, mitigation is far from instantaneous. Even after you perform all the legwork to identify a compromised device, for example, your work isn’t over. If the device is an executive’s iPad, for example, you have to get hold of that user, explain the situation, and walk him or her through mitigation actions. If you’re doing all this while malware is propagating through your environment, you’re already too slow. By combining your SIEM or TD solution with contextual data and mitigation capabilities, you can go from detect to identify to quarantine, literally in seconds.
- **Contain threats before they spread:** Along the same lines, integrating contextual data and policy enforcement with your SIEM or TD platform insulates your environment from the most virulent threats. You may not be able to stop the nastiest attacks from finding their way to a network-connected device. But you can identify and block those attacks before they start infecting large segments of your network.
- **Gain total visibility:** By combining your SIEM or TD platform with more precise contextual data, you gain much more visibility into your environment. Any user, any device, any place in the environment is clearly identifiable from a single console. And, with the ability to create custom analytics for the highest-risk areas (personal mobile devices, guest users, users with access to the most sensitive data, etc.), you can keep a closer eye on those areas where it matters most. More visibility brings more control.

Looking Ahead

The ability to have security event analytics, contextual visibility, and remediation all in one place provides a powerful threat defense capability. Really, it's an essential capability in modern network environments. In a world where applications are virtualized, users are mobile, and network devices run the gamut from corporate-owned to user-owned, from server to desktop iPad to smartphone, comprehensive contextual visibility is the only way to stay ahead of threats.

But we can expect even more powerful network defenses as new tools supplement and integrate with these capabilities. Cisco is leading the way in these emerging security innovations, including:

- **Cisco TrustSec security group tagging and management paradigms,** which allow you to logically segment networks from the user or device all the way to the virtualized application in the data center, according to security policy. *Read more about TrustSec on page 6.*
- **Security information clearinghouses such as the Cisco Platform Exchange Grid (pxGrid)** that enable collaboration across all the security, policy, and network management platforms in your network—and even across devices from multiple vendors—without the need for platform-specific APIs. *Read more about pxGrid on page 7.*
- **Open security ecosystems** that expose contextual information and capabilities throughout your network and allow third-party partners to develop innovative threat defense solutions.

Conclusion

Drawing on intelligence throughout the network infrastructure, Cisco security solutions, and third-party innovators, Cisco is expanding the boundaries of what's possible in network threat defense and regulatory compliance. Cisco ISE integrates with SIEM and TD platforms to provide the relevant context for any network threat. With these expanded capabilities, you can answer the "who," "what," and "where" questions to properly assess and prioritize suspicious network activity, and then immediately take action.

The bad guys will always be out there. But with a new generation of security techniques and innovations, we can neutralize many of their most effective weapons.

For More Information

View Video, http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11640/protect.html (03:34min)

Cisco Identity Services Engine: Relevant Context and Centralized Policy Enforcement

Context is king when it comes to accurately assessing security events. But how do you get it? Cisco ISE provides the answer. It delivers:

- **A central point of user and device context and policy for your entire network:** The tools to identify and profile devices, authenticate devices and users, and enforce policy decisions used to exist in separate solutions that had to be manually tied together, a process that was not always smooth or straightforward. Now, Cisco ISE, working with Cisco Unified Access [http://www.cisco.com/en/US/netsol/ns1187/index.html] to create "One Policy," gives you all of these services in a single appliance.
- **Embedded network-wide profiling and authentication intelligence:** Rather than install separate appliances to detect and profile devices connecting to the network, Cisco ISE draws on intelligence from the network itself. Cisco ISE communicates with profiling sensors in all network switches and wireless controllers to profile device types, track the session state of all devices, and enforce policies in a single integrated system.
- **Simplified, policy-controlled BYOD onboarding:** Cisco ISE provides integrated onboarding services for mobile devices, allowing you to configure and provision profiles to all types of supplicants (iPhones, iPads, laptops, etc.) and grant access based on user and device context.

To learn more about Cisco ISE, visit http://www.cisco.com/go/ise**.**

Cisco TrustSec Segmentation: Policy-Based Network Traffic Controls

Implementing and maintaining a network security policy may sound straightforward in theory. In practice, it's an onerous, time-consuming task. To implement a security policy, network engineers must use the arcane language of virtual LANs (VLANs), access control lists (ACLs), and firewall rules, translating seemingly simple guidelines into a vast web of complex instructions to block or forward traffic to and from specific IP addresses. The Cisco TrustSec solution offers a better alternative.

Cisco TrustSec technology draws on a centralized security policy from Cisco ISE. It provides a network-wide security tagging mechanism that lets you segment all wired and wireless network traffic without VLANs. Based on proven traffic-tagging technologies embedded in Cisco switching, routing, wireless LAN, and firewall products, it lets you control access to, and protect the resources of, enterprise and data center networks.

Cisco TrustSec enforcement policies recognize users, devices, and machines by their contextual identity; assign them to a security group; and control their access to and from any other endpoint or resource in the network. You can use this Cisco TrustSec tagging technology to forward traffic; to unlock resources for access; and, deploy it as a virtual firewall, to help prevent malware exploitation between endpoints and resources. Ultimately, you can segment and protect your network with policy-based access without the complexity of managing ACLs and firewall rules.

To learn more about Cisco TrustSec, visit www.cisco.com/go/trustsec.

Cisco Platform Exchange Grid (pxGrid): Getting the Right Information to the Right IT Platform

Protecting a modern network requires numerous IT tools and platforms, many of which operate as unconnected "silos" of information. Although these tools can be effective in their own domain, they can't easily share their information with other tools, nor can they consume information they need from other systems.

In the past, any kind of data sharing meant using a single-purpose, platform-specific API. But today, when you have a large number of platforms running simultaneously, this one-off approach limits your ability to achieve ubiquitous visibility and threat response capabilities.

Cisco pxGrid enables multivendor, cross-platform network system collaboration. It brings together the many diverse parts of an IT infrastructure, including security monitoring and detection systems, network policy platforms, asset and configuration management, identity and access management platforms, and virtually any other IT operations platform. As a result, security devices and Cisco ecosystem partners can use pxGrid to share relevant, customizable contextual information wherever it's required.

The Cisco pxGrid suite of context-sharing and network-control capabilities enables network defense systems to address more use cases, undertake their functions more effectively, and extend their reach throughout the network infrastructure.

To learn more about Cisco pxGrid, visit
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11640/at_a_glance_c45-728420.pdf

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 01/14