Detect and Thwart Insider Threats

When former National Security Agency contractor Edward Snowden leaked classified information to the mainstream media, it brought the dangers posed by insider threats to the forefront of public consciousness. And not without reason.

Insider threats are one of the hardest threats to detect. And they can compromise large swaths of sensitive data. A report by Forrester Research suggests that insiders are the top source of data breaches: 36 percent of breaches stem from the accidental misuse of data by employees, and 25 percent result from abuse by a malicious insider.

The danger is especially apparent in government organizations that regularly deal with classified information. Because of the severe impact of the loss of classified data, many of these organizations are under federal regulations that require them to monitor, mitigate, and document any insider threat activity.

Whether it is a negligent employee, a malicious insider, or an outsider who compromises legitimate credentials, many organizations still do not have a security plan in place that effectively addresses attackers from within. The best way to combat insider threats is through early detection. To do so, security personnel need pervasive network visibility and in-depth behavioral analytics.

Turn the Network into a Sensor with Visibility and Behavioral Analytics

By virtue of their privileged status, insiders are often able to circumvent many security measures. Outside attackers have to worry about gaining access to the protected networks in the first place. Insiders are willingly given access to sensitive data. With the rise of the bring-your-own-device (BYOD) workplace, in which personal devices are increasingly used for work, employees may even be able to access the data from home using their smartphone. To combat these threats, defenders need to approach security differently.

[1] Forrester Research Report, Understand the State of Data Security and Privacy: 2013 to 2014, October 2013

© 2016 Cisco and/or its affiliates. All rights reserved.

Detect and Thwart Insider Threats

To detect insider threats, you need to employ comprehensive internal network visibility and security analytics. One approach is to use Cisco® Stealthwatch, which collects and analyzes large quantities of NetFlow and other types of security data. With Stealthwatch, you can harness your existing network infrastructure to identify behaviors that could signify an insider threat.

For instance, a user who collects an abnormally large amount of data or attempts to access restricted network segments could be preparing to exfiltrate sensitive information. Likewise, a user that suddenly sends a large volume of traffic to the local printer could be making hard copies of confidential files in hopes of avoiding perimeter security. Stealthwatch can detect the lateral movement associated with insider threats or external attacks proliferating throughout the network.

Without internal network visibility, it is difficult to identify these activities or even investigate them after a breach has happened. But visibility is only half of the equation. Without a way to store, organize, and transform data into actionable intelligence, it is nearly impossible to translate visibility into real-world benefits.

Stealthwatch's robust analytics can quickly process network traffic data and identify suspicious and anomalous behavior. It does this primarily by collecting NetFlow and other network metadata from preexisting devices. It thus effectively transforms the network into a powerful security sensor. You gain end-to-end visibility without the prohibitive costs associated with deploying monitoring devices.

When the data is collected, Stealthwatch trims it down to streamlined data objects. It then uses proprietary algorithms to determine what activity is taking place. It highlights any activity that could represent a threat (Table 1), so security personnel can mitigate it before significant damage is done.

Aligning with Federal Insider Threat Regulations

Federal agencies feel great urgency to prevent insider threats. They must protect the security of classified information and ensure compliance. Stealthwatch, with its advanced anomaly detection and visibility into NetFlow activity, can help government organizations comply with policies pertaining to insider threats. Stealthwatch addresses regulations such as Executive Order 13587 and Intelligence Community Standard 500-27, by both monitoring network traffic and retaining an information-rich audit trail.

The Department of Defense (DOD) and other U.S. government agencies are mandated to build programs that protect against insider threats. In addition, the National Industrial Security Program Operating Manual requires thousands of contractors to have an insider threat program. Unfortunately, according to the Insider Threat Task Force of the Intelligence and National Security Alliance (INSA) Cyber Council, many such organizations have no insider threat program in place, and most of the organizations that do have serious deficiencies.

Over the past decade, more than 120 cases of malicious insider crime have been Recorded involving classified national security information.[2]

[2] CMU, http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_427430.pdf, April 2014

© 2016 Cisco and/or its affiliates. All rights reserved.

Detect and Thwart Insider Threats

Reducing the Time to Detect a Threat with Contextual Awareness

Even if you have internal network visibility, you may not see an insider threat. Attackers can hide their activity by splitting it up among multiple devices and time frames. Identifying suspicious behavior doesn't help much unless you can tie it to a specific user. In fact, according to a Ponemon Institute study, the lack of contextual information from security tools is the biggest hurdle to determining whether insiders pose a threat.[3]

Table 1. Anomalous Behavior That May Represent a Threat

Activity	Description
Unauthorized access	A user attempts to access prohibited resources on the network.
Policy violations	An employee uses services that are in violation of organizational policies and that may be intended to bypass organization monitoring.
Internal reconnaissance	A user scans the network. (Before insiders can extract data, they must inventory it.)
Suspect data hoarding	A user begins collecting abnormally large amounts of data.
Target data hoarding	A user extracts large amounts of data from a specific host.
Suspect data loss	A privileged user sends abnormal amounts of data outside the network, signifying potential data exfiltration.

Case Study: Stealthwatch improves Federal Network Security

In light of increasingly sophisticated and high-profile cyber attacks, it became clear to one federal agency that implementing the minimum requirements to comply with federal regulations was no longer enough to protect its critical assets.

The agency benefits from Stealthwatch's automated monitoring, baselining, and alarming functions. Not relying on signature updates, Stealthwatch uncovers sophisticated zero-day attacks and also detects insider threats including policy violations, network misuse, device misconfigurations, and data leakage.

Advanced security capabilities in Stealthwatch streamline troubleshooting and dramatically improve protection. They also boost compliance efforts and assist with network forensic analysis for incident investigations. These capabilities include:

- **Comprehensive, continuous monitoring** of the entire network to enhance visibility
- **Behavioral-based anomaly detection** for fast troubleshooting of internal and external threats without requiring signature updates to detect attacks
- **The concern index** to automatically prioritize the top security issues facing an organization
- **Automatic mitigation** to give IT administrators the option of quickly containing security problems
- **The worm tracker**, which visually graphs the spread of malware throughout the network to provide instant visibility into its scope and impact
- **Host-group locking** to limit communication with sensitive systems
- **Identity awareness** to pinpoint the exact users responsible for (or affected by) issues
- **Network forensic analysis** to enhance investigation

Above all, Stealthwatch provides the additional "eyes and ears" sought by this organization to make continuous process improvements for securing its confidential assets. The system augments existing security deployments to achieve earlier detection and a more prompt and agile response to incidents.

Read the full case study: www.lancope.com/csusfed

[3] Ponemon Institute Research Report, Privileged User Abuse and the Insider Threat, May 2014

© 2016 Cisco and/or its affiliates. All rights reserved.

Detect and Thwart Insider Threats

Stealthwatch is able to provide multiple layers of security context. Administrators gain a clear picture of user activity and can make informed decisions. This context includes the following:

- **User identity:** Tying network activity to the responsible user is critical to identifying insider threats.
- **Device awareness:** Device information helps identify unauthorized or insecure devices, as well as quickly identify machines that may be compromised.
- **Application-level visibility:** The ability to see which applications are in use can help pinpoint attacks and malicious programs.
- **Threat-feed data:** This data helps identify machines or users who have been interacting with known malicious hosts.

Advanced attacks can take up to a year or more to discover. In the meantime, they lurk on the network and wreak havoc. Additional layers of security context can significantly reduce the time to detection (TTD) for a wide range of threats.

Discovering the Scope of an Attack Through Forensic Investigations

When a security threat is identified, it is vital to be able to investigate how your network was compromised and, more importantly, what data may have been obtained. This is difficult to do unless you have a record of network transactions.

NetFlow itself can produce large amounts of data that can be difficult to store effectively. Stealthwatch, however, can streamline flows and reduce data requirements significantly without sacrificing important information. Consequently, Stealthwatch users can store months or even years of traffic data to facilitate more comprehensive forensic investigations.

Stealthwatch is highly scalable to meet the needs of even the largest organizations. It analyzes up to 240,000 flows per second (fps) per collector, or 6 million fps total. The Stealthwatch management console provides an intuitive user interface. It is easy to query flow records with a variety of parameters and to look at elements that are pertinent to the investigation.

Today's organizations face a wide spectrum of threats, but few are prepared to deal with attacks from insiders. Stealthwatch excels at detecting insider threats through the use of in-depth network visibility and context-aware security analytics. You can monitor, detect, analyze, and respond to the full range of threats before they lead to irreparable damage.

For More Information

To learn more about Cisco Stealthwatch, visit: http://www.cisco.com/c/en/us/products/security/stealthwatch/.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

(08/23/16-r02)