Threat Hunting
Find the threats. Learn from them. Strengthen your security.

Organizations of all sizes and types are investing in sophisticated security solutions and talent, yet major data breaches remain a regular occurrence.

Appearance vs. Reality
Investments in firewalls, intrusion detection systems, spam filters, anti-malware solutions, and advanced next-generation security tools present the appearance of a secure organization, but the reality is that attackers know how to exploit or circumvent those defenses, and often work in the shadows of your network for months before a compromise or breach is even detected.

Even with security tools and experienced staff in place, it’s still difficult to detect threats. The sheer volume of event data is overwhelming, and security teams are so busy reacting to alerts and trying to separate the signals from the noise that there’s no time left to proactively improve security and identify existing compromises before they become massive data breaches.

Have You Been Compromised?
Have you been breached? is a simple question. But are you able to answer this question with confidence?

Attackers are patient and clever. They find and exploit weaknesses to gain entry into your organization—the first stage of an attack. They then wait quietly, blending in with normal activity for weeks or months before they strike—successfully exfiltrating your data for days, weeks, or months before you realize you have a breach on your hands.

How can you defend your organization against these types of attacks? If you don’t have the right solution in place to continuously monitor your network and proactively identify suspicious or malicious activity, detecting whether or not your data has already been stolen can be a nearly impossible task.

SecurityCenter Continuous View Threat Hunting Capabilities
- **Active Scanning** - Periodically scan assets to determine their level of risk to the organization
- **Intelligent Connectors** – Leveraging your other security investments, integrate additional security data to improve context and analysis
- **Agent Scanning** – Instantly scan assets without the need for credentials
- **Continuous Listening** – Monitoring network traffic in real-time provides information on which assets are connected to the network and how they are communicating
- **Host Data** – Actively monitoring host activities and events, including who is accessing them and what is changing

Many organizations find themselves in the unfortunate position of learning about a data breach when a financial institution or the FBI calls to investigate fraudulent activity. Are you breached right now? Can you answer that question with even a remote degree of confidence? If you don’t have the tools and resources in place to continuously monitor your network and proactively identify suspicious or malicious activity, you can’t say for sure that your data hasn’t already been stolen.
Security Requires Complete Visibility

Threat hunting feels like looking for a needle among needles in a huge haystack. In today's threat landscape, you need a precision magnet to find and capture the needles that pose the greatest threat to your network or data. Tools that aggregate logged events, monitor for suspicious user behavior, or analyze huge amounts of data to detect anomalous patterns or events all promise to help address this challenge; however, they often lack key elements you need to have a complete view of your network or they require staff expertise in areas like packet analysis, malware, and threat intelligence.

Without comprehensive and continuous visibility across all of the platforms and devices in your environment, you can't be sure that you aren't already breached. More importantly, you need the tools to provide context—to be able to connect the dots to make sense of the mountain of security data you have—so you can focus action on the events that matter most and identify a compromise before the attacker is able to get sensitive data out of your environment.

Another challenge when it comes to detecting a compromise before it becomes a breach is persistence. Attackers attack constantly. Periodic scans aren't sufficient because attacks aren't periodic. You need to have continuous security monitoring to be vigilant in hunting suspicious behavior and indicators of compromise in your environment.

Proactive Threat Detection & Identification

Tenable SecurityCenter Continuous View (SecurityCenter CV) enables you to quickly start taking the right steps to proactively address compromises before they become breaches.

Tenable continuously collects indicators of compromise (IOCs) from leading commercial threat intelligence vendors that enable you to identify emerging threats in near real-time without any additional licensing or configuration costs. SecurityCenter CV also automatically creates a baseline of normal activity and includes built-in anomaly detection.

*With Tenable, you can identify and measure divergence from normal activity patterns across all types of collected event data with no additional licensing fees or complex configuration.*

SecurityCenter CV can also correlate indicators and other security events to chain potentially suspicious activities together from across your environment, uncovering complex, advanced threat conditions from commonly collected events and data.

Scale Your Threat Hunting Team

All threats are not created equal. You need context to answer relevant security questions, prioritize risk, and make better decisions. Tenable SecurityCenter CV gathers information from a broad spectrum of sources, including active scanning, passive scanning, intelligent connectors, agents, and host activity data to facilitate the decision making process.

In addition, the Tenable service includes a team of security professionals that constantly monitor a variety of threat intelligence sources and correlate industry trends, emerging threats, and common frameworks on your behalf. This intelligence helps you automatically know—based on your current data set—if you have ever been impacted so you can address high-priority threats quickly.

As a dedicated extension of your security team, Tenable's trusted advisors are always working behind the scenes as a key element of your security program. We give you a powerful program that you can use to secure your organization's growth with confidence. You get better business outcomes and a scalable security team that will increase your team’s productivity and reduce the time and money needed to invest in organizational security training.

Hunt for Threats with Confidence

The array of information that Tenable collects—especially from passive network scanning—ensures that SecurityCenter CV is always diligently watching your assets and data for suspicious or anomalous activity.

The Tenable Research library of curated dashboards, reports, and assurance report cards (ARCs) illustrates security information in an actionable format designed to meet a variety of information security standards and best practices.

Uncertain where to begin looking? Jump-start your hunt with dashboards. Our library of dashboards illuminate common indicators of compromise and suspicious activity to get you started. Their highly customizable nature enables you to fine-tune detections and pinpoint exactly where threats are lurking in your environment.

Stay One Step Ahead on the Hunt

Don’t get caught off guard—by attackers, by your board, or by your own manager. You should be able to confidently answer the question, “Are we breached?” and you should be the first—rather than the last—to know when a compromise occurs.

Tenable gives you the tools you need to continuously monitor for and proactively identify compromises before they become data breaches. Tenable SecurityCenter CV helps you distill the relevant security threats from the overwhelming security noise so you can quickly see suspicious patterns across your environment and take informed action.

When you choose Tenable and our team of security experts, you’ll make appearance versus reality a solution rather than a way to describe a significant problem, and you’ll achieve a level of security effectiveness only realized with a scalable and comprehensive approach to security.

About Tenable

Tenable delivers comprehensive security solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization.

Transform security with Tenable, the creators of Nessus and pioneers of continuous monitoring.

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact

Copyright © 2016. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. SecurityCenter Continuous View and Passive Vulnerability Scanner are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JAN282016-V3