Solution Brief

Tenable and ThreatConnect

Detect Advanced Attacks With Continuous Monitoring and Threat Intelligence

The Challenge

Security operations teams do not have enough context around their threat intelligence to detect and prioritize advanced attacks. Having that context, in terms of indicators of compromise relevant to an incident, can guide you with accurate forensics analysis and provide actionable next steps to respond to intrusions and breaches. Security teams are taking a proactive approach to threat intelligence, maintaining their own threat profiles with historic knowledge of specific threats, and sharing that knowledge with others who are also affected by increasingly sophisticated and complex threats.

Security teams face the following challenges to protect their enterprises from advanced targeted attacks:

- Security data is not shared between IT and Security Operations teams, making it impossible to connect the dots between events and related threats
- Indicators often do not have enough context to help detect and prioritize incidents
- Results of forensics analysis are not visible and integrated with response and defense mechanisms
- Inability to maintain historic knowledge of incidents, threats and associated indicators within a single source

The Solution

This joint solution brings together the industry leading vulnerability, threat and compliance management capabilities from Tenable™, and leverages unique threat intelligence in the ThreatConnect™ platform, to provide continuous visibility into advanced attacks that escape traditional security solutions.

The Tenable products used in the joint solution include:

- Nessus® active scanner, which provides patch, configuration and compliance auditing for known vulnerabilities and threats.
- SecurityCenter®, which provides the centralized console to manage multiple Nessus scanners and provide advanced analytics, alerts, dashboards and reports for security and compliance.

ThreatConnect provides the most advanced, collaborative threat intelligence platform – combining threat data collection, analysis, collaboration and expertise into a single platform. ThreatConnect enables the security community to develop a more complete understanding of threats targeting their organizations.

Tenable SecurityCenter and Nessus products, programmatically import threat indicators (e.g., Host, Address, Email-address, URLs, Files) from ThreatConnect to dynamically create watchlists of these suspicious assets and perform audits and event analysis to accurately detect advanced attacks. By continuously monitoring for relevant threat intelligence in the ThreatConnect platform gathered from a community of over 2,000 security researchers, analysts and organizations, our joint customers can stay up to date on global security trends affecting you and your industry.

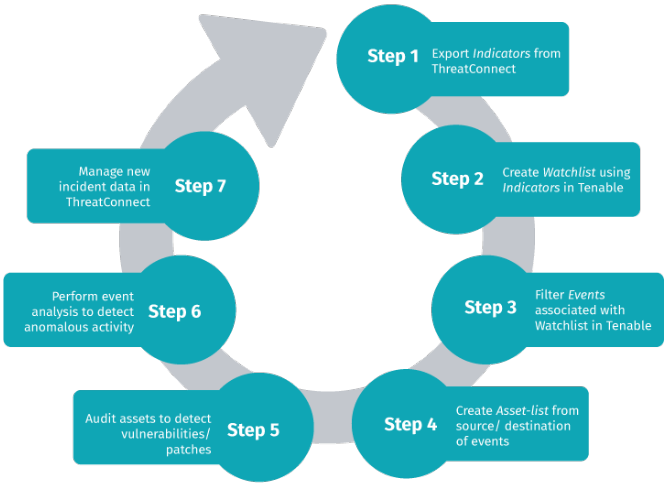
Components:

- Tenable SecurityCenter management console
- Tenable Nessus vulnerability scanners
- ThreatConnect threat intelligence platform

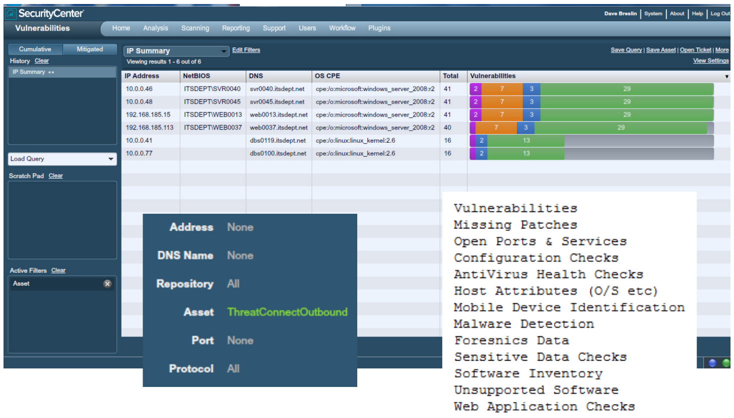
Benefits:

- Leverage global threat intelligence data from the ThreatConnect platform
- Dynamically discover new threats by continuously monitoring for indicators in assets using watchlists
- Take action in Tenable to audit for vulnerabilities in assets exploited by these threats and patch them to reduce risk
- Use knowledge from past incidents detected with Tenable to discover new related indicators within ThreatConnect

How It Works


Step 1
Export *Indicators* from ThreatConnect
Step 2
Create *Watchlist* using *Indicators* in Tenable
Step 3
Filter *Events* associated with Watchlist in Tenable
Step 4
Create *Asset-list* from source/ destination of events
Step 5
Audit assets to detect vulnerabilities/ patches
Step 6
Perform event analysis to detect anomalous activity
Step 7
Manage new incident data in ThreatConnect

Threat intelligence relevant to a specific customer can be exported from the ThreatConnect cloud platform to the Tenable solution installed at the customer site. The appropriate threat intelligence data (IP address, host-name, email address, URL, filename) can be used to create a “watchlist” that will be monitored in Tenable. Then you can filter for events and gather other source/destination assets that may be compromised by lateral movement of malware. You can perform audit and event analysis on these assets to detect vulnerabilities and malware activity, to accurately detect intrusions and breaches. Relevant indicators discovered can then be uploaded back into ThreatConnect for correlation for knowledge management and correlation with related indicators.



Viewing results 1 - 6 out of 6

IP Address	NetBIOS	DNS	OS CPE	Total	Vulnerabilities
10.0.0.46	ITSDEPT\SVR0040	svr0040.itsdept.net	cpe:/o:microsoft:windows_server_2008:r2	41	2 7 3 29
10.0.0.48	ITSDEPT\SVR0045	svr0045.itsdept.net	cpe:/o:microsoft:windows_server_2008:r2	41	2 7 3 29
192.168.185.15	ITSDEPT\WEB0013	web0013.itsdept.net	cpe:/o:microsoft:windows_server_2008:r2	41	2 7 3 29
192.168.185.113	ITSDEPT\WEB0037	web0037.itsdept.net	cpe:/o:microsoft:windows_server_2008:r2	40	7 3 29
10.0.0.41		dbs0119.itsdept.net	cpe:/o:linux:linux_kernel:2.6	16	2 13
10.0.0.77		dbs0100.itsdept.net	cpe:/o:linux:linux_kernel:2.6	16	2 13

Address	None
DNS Name	None
Repository	All
Asset	ThreatConnectOutbound
Port	None
Protocol	All

```
Vulnerabilities
Missing Patches
Open Ports & Services
Configuration Checks
AntiVirus Health Checks
Host Attributes (O/S etc)
Mobile Device Identification
Malware Detection
Forensics Data
Sensitive Data Checks
Software Inventory
Unsupported Software
Web Application Checks
```

Integration Benefits

When selecting an ecosystem for detecting and preventing threats to your network using threat intelligence, you need a combination of products that provide quality and relevant threat intelligence, and allow you to manage, grow and quickly leverage that intelligence defensively through powerful integrations.

Your solution should be able to leverage relevant threat intelligence to continuously monitor for suspicious network activity using watchlists, and accurately identify vulnerabilities in assets that can be exploited by these new advanced threats. This situational awareness should be used to patch vulnerabilities and reduce overall business risk and improve security posture of IT infrastructure.

The benefits of a combined Tenable and ThreatConnect solution are compelling:

- Seamlessly leverage global threat intelligence into SecurityCenter and Nessus for situational awareness and discovery of new threats
- Discover new threats by continuously scanning for indicators in assets using dynamically created watchlists in Tenable
- Take action in Tenable to audit for vulnerabilities in assets exploited by these threats and patch them to reduce risk
- Use knowledge from past incidents detected with Tenable to discover new related indicators within ThreatConnect
- Manage knowledge of threat and incident history in ThreatConnect

About ThreatConnect

ThreatConnect, Inc. provides industry-leading advanced threat intelligence software and services, including ThreatConnect®, the most comprehensive Threat Intelligence Platform (TIP) on the market. ThreatConnect delivers a single platform in the cloud and on-premises to effectively aggregate, analyze and act to counter sophisticated cyber-attacks. Leveraging advanced analytics capabilities, ThreatConnect offers a superior understanding of relevant cyber threats to business operations. To register for a free ThreatConnect account, or to learn more about our products and services, visit: threatconnect.com.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

tenable™

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