Closed-Loop Security with Ticketing System Integration

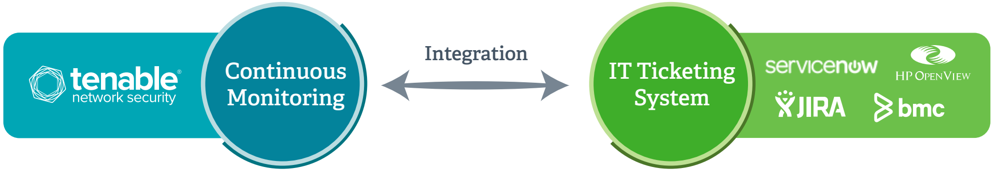
Tenable Offers Flexible Service Desk Integration to Automate Remediation

Key Challenges

Upon detection of critical vulnerabilities and security risk, IT teams must notify multiple stakeholders so that remediation process is promptly triggered. The key to success lies in automating this process by integrating with existing service desk solutions.

Enterprises can respond and timely mitigate issues with solutions that:

- Offer a flexible architecture that works with deployed ticketing or service desk software such as Jira, ServiceNow, and others.
- Allow the ability to customize notifications per customer's workflow.
- Offer bi-directional communications for creating/updating service desk tickets.
- Support closing of tickets upon verification of successful mitigation



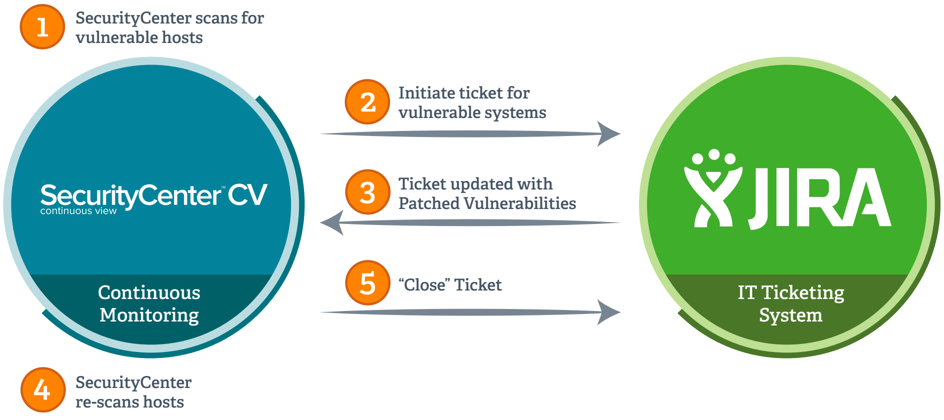
Solution Overview

Tenable Network Security offers a flexible solution that not only provides incident notification and alerting, but also integration with service desk and ticketing systems for tracking by appropriate response and remediation teams. This ensures a closed-loop management and automated workflow for processing security incidents and tracking their status throughout the mitigation process.

Unlike other solutions, the Tenable architecture also validates the effectiveness of response actions, such as the patching of vulnerabilities, via subsequent scan results. This ensures that issues are indeed resolved before tickets are closed.

How it Works

As an example, the integration with JIRA allows bi-directional communications for a complete view of detection, remediation, and verification of security issues within the organization. This takes place in three phases: Import, Rescan, and Close.


1 SecurityCenter scans for vulnerable hosts
SecurityCenter CV continuous view
Continuous Monitoring
2 Initiate ticket for vulnerable systems
3 Ticket updated with Patched Vulnerabilities
5 "Close" Ticket
JIRA
IT Ticketing System
4 SecurityCenter re-scans hosts

Solution Components:

- Tenable SecurityCenter™ Continuous View
- Tenable SecurityCenter™

Key Benefits:

- Simplifies IT workflow by integrating with existing ticketing system
- Eliminates manual overhead by automatically creating service desk tickets after vulnerability scanning
- Decreases time to initiate mitigation by identifying list of critical issues for remediation
- Facilitates better use of IT resources by prioritizing vulnerable systems
- Allows customization based on customer specific triggers and requirements
- Eliminates inconsistencies by updating ticket status after security issues are resolved

Phase 1: Import

1. SecurityCenter CV performs security assessment to detect vulnerabilities on systems (endpoints, servers, databases, web applications, etc.).

2. The integration script queries SecurityCenter CV for vulnerable hosts. For each vulnerable host a parent ticket is created in JIRA and a subtask is created for each vulnerability identified on the host.

Phase 2: Rescan

1. Resolved tickets are placed in the “fixed” state within JIRA.

2. The integration script identifies all tickets in “fixed” state and initiates re-scans for them on a pre-defined schedule (for example, every night).

Phase 3: Close

1. For each “fixed” ticket in JIRA the integration script queries SecurityCenter CV to verify the vulnerability is mitigated.

2. If the vulnerability is mitigated, the JIRA ticket is moved to the closed state.

3. If the vulnerability is not mitigated, the JIRA ticket is moved to the “unfixed” state.

4. All “unfixed” tickets remain open and should be investigated by IT team to determine root cause.

The above illustrates the integration and workflow between SecurityCenter CV and JIRA. Tenable Professional Services can develop a custom integration for other ticketing systems.

Benefits

Solutions that offer closed-loop security assessment by integrating with major ticketing systems relieve the burden of manually managing and tracking remediation and response. They decrease time to initiate mitigation actions and facilitate better use of IT resources by prioritizing critical issues for immediate resolution. Advanced solutions, such as Tenable’s SecurityCenter Continuous View, also offer the additional advantage of bi-directional communications with ticketing systems to enable automated updates back to security assessment teams and validate remediation effectiveness.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world’s largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, please visit tenable.com.

tenable® network security

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