SOLUTION BRIEF

Tenable and Fortinet

Improve Incident Response with Security Orchestration, Automation, and Response

Executive Summary

The Fortinet integration with Tenable combines Tenable's Cyber Exposure insights with Fortinet's FortiSOAR for complete visibility into an organization's security infrastructure and attack surface. The solution enables automated workflows as well as improved and accelerated security incident response.

Business Challenge

Organizations struggle with focus and upkeep on security tools within their security environment. These gaps put them at greater risk and continually grow the threat landscape. Without integrating Tenable's vulnerability data into the Fortinet security orchestration, automation, and response (SOAR) platform, organizations are left without a way to utilize automated workflows and maximize resources for accelerated incident response.

Solution

The Fortinet integration with Tenable combines Tenable's Cyber Exposure insights with Fortinet's FortiSOAR for complete visibility into an organization's security infrastructure and attack surface. Security and IT teams are provided with management insights, pre-configured workflows, and real-time dashboards to automate time-intensive, manual processes for streamlined incident response. Organizations can utilize the integration to represent and correlate vulnerabilities and assets, and scan data from Tenable combined with Fortinet's SOAR engine for improved incident response.

Features

For Tenable.io you can:

- Get a list of available scans
- Launch a scan
- List assets of a given scan
- Get plugin details
- Get all vulnerabilities
- Get all assets

Key Benefits

- Improve incident response time
- Enrich incident response with vulnerability context
- Improve processes with configured workflows
- Automate your teams' manual tasks
- Connect Tenable to disparate security tools

Value

The Fortinet integration for Tenable provides the ability to:

- Provide predefined parameters for running vulnerability management scans without requiring knowledge about vulnerability management configuration and internal network infrastructure
- Define approval processes for running one-off infrastructure vulnerability scans
- Allow for the creation of automated workflows across security tools
- Centralize your vulnerability insights by viewing a single dashboard

FORTINET Fabric-Ready

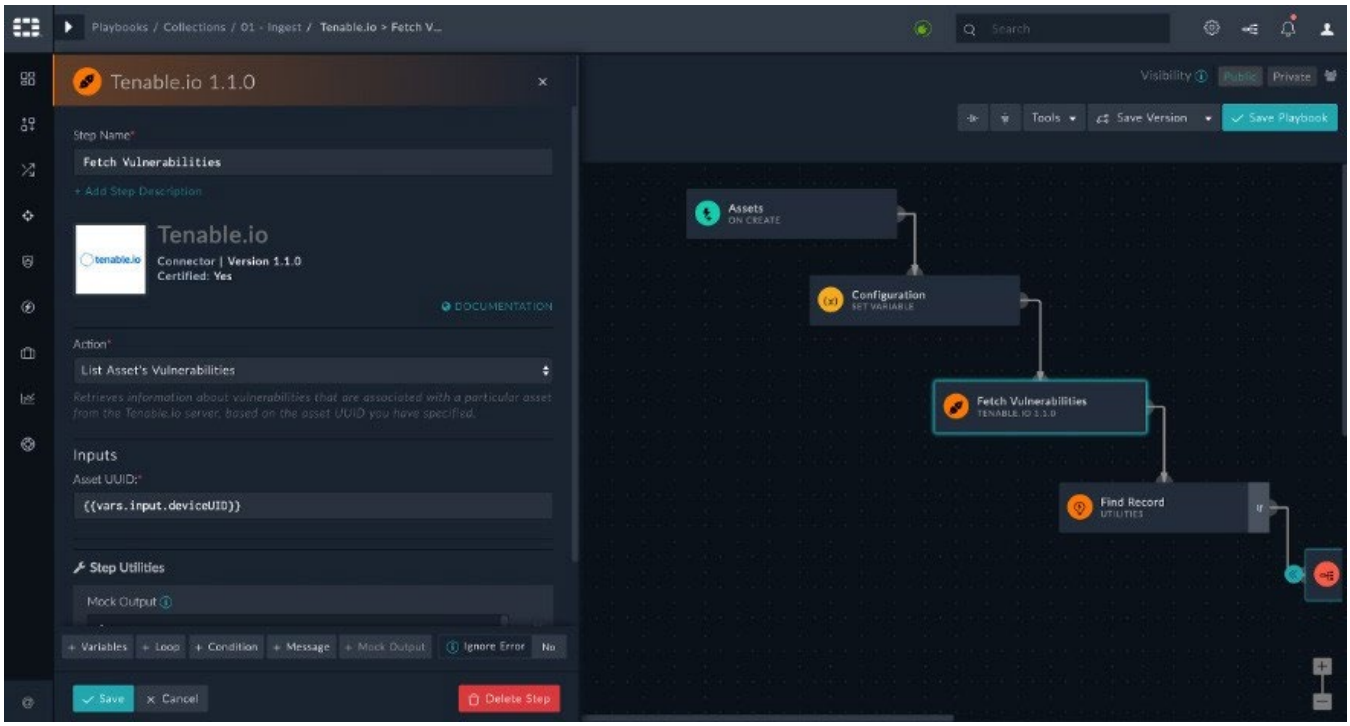

Figure 1: The diagram shows Tenable vulnerability findings supplementing Fortinet's SOAR platform that allows security and IT teams to have full visibility into their security infrastructure and attack surface.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. More than 455,000 customers worldwide trust Fortinet to protect their businesses. Learn more at www.fortinet.com.

Installation and Configuration Documentation

https://help.cybersponse.com/support/login

https://www.tenable.com/products/tenable-io/evaluate

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 15, 2020 11:12 PM

D:\Fortinet\Solution Briefs\grey solution briefs\Tenable\sb-FA-tenable-and-fortinet-152020

703055-0-0-EN