INTERGRATION BRIEF

Understand the Full Risk Potential by Including Vulnerability Data in Your Response.

Gather critical, up-to-date vulnerability data to understand the full risk an incident may pose with Tenable and IncMan SOAR.

DFLABS.COM

Automate.
Orchestrate.
Measure.

tenable | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Vulnerability data is crucial to protecting a company's assets. Without this data and the ability to utilize it during a potential incident, an organization's threat landscape would be nearly impossible to defend.

DFLabs integration with Tenable expands an organization's ability to protect their valuable assets by allowing network defenders to operationalize this data to stay ahead of an attack. In doing so, this integration will also help break down the barriers between vulnerability and security teams allowing them to operate as one cohesive defensive force.

Orchestration and Automation are critical components in responding effectively and efficiently to a cyber security incident.

The Problem.

Unhandled vulnerabilities continue to plague organizations and leave their operations open to a potential attack. Contributing to this threat is the siloing of teams responsible for vulnerability remediation and the security teams tasked with protecting an organization's assets.

Combining these common issues could be a recipe for disaster. Vulnerability teams are in the dark regarding what assets are under attack and security teams are unaware what systems have yet to be patched in the critical first moments of an incident. The inability to correlate this information and collaborate with disperse teams hinders an organization's ability to better prioritize patching and remediation efforts.

CHALLENGES

- Unhandled vulnerabilities leave organizations exposed to potential attacks
- Siloing of teams makes collaboration difficult
- Inability to prioritize and utilize vulnerability data during an incident reduces a security team's visibility into the entirety of a suspicious event

DFLabs and Tenable Solution.

The integration between DFLabs IncMan and Tenable closes the gap between security and vulnerability teams by providing a comprehensive look into an environment as a whole. By providing network defenders the most up to date vulnerability information, they can quickly assess the severity of incident and alert vulnerability and IT teams of a high priority issues within the infrastructure.

This collaborative partnership not only allows containment of a high priority incident to happen in real-time, but also identifies what vulnerabilities are actively being targeted so support teams can patch and remediate efficiently.

- Real-time vulnerability data available for incident
- Breaking down of siloed environments to allow collaboration between disperse teams
- Vulnerability prioritization based off of active attack vectors

Automate.
Orchestrate.
Measure.

About Tenable.io.

Tenable.io provides a risk-based view of your entire attack surface- from IT to cloud and containers. Managed in the cloud and powered by Nessus technology, Tenable.io provides the industry's most comprehensive vulnerability coverage with the ability to predict which security issues to remediate first.

It's the complete end-to-end vulnerability management solution.
With Tenable.io organizations will be able to quickly identify, investigate and prioritize vulnerabilities.

About IncMan.

DFLabs IncMan Security Orchestration, Automation and Response platform automates, orchestrates and measures security operations and incident response tasks including threat validation, triage and escalation, context enrichment and threat containment. IncMan uses machine learning and Rapid Response Runbooks (R3 Runbooks) as a force multiplier that has enabled security teams to reduce average incident resolution times by 90% and increase incident handling by 300%.

Use Case.

An IDS alert is received indicating a current vulnerability exploit attempt has been observed towards an organization's Web server. IncMan receives the alert and begins to gather system information for the affected Web server.

The organization's directory services platform as well as their EDR solution is queried for the system information including OS type and version. Once this information is gathered, IncMan pulls the list of scanning templates from Tenable.io. This information is fed into IncMan to automatically generate a vulnerability scan against the affected Web server.

Upon completion of the vulnerability scan, IncMan issues a User Choice action. This action will pause the incident's runbook to allow for the security team to review the results of the previous Runbook actions. If the system is found to have an open vulnerability associated with the exploit attempt, the security analyst will select a positive result which will automatically generate an email notification to the Vulnerability and Systems team and open a new ticket within the organization's ticketing system. Once these notifications are sent, IncMan issues a request to the EDR solution to tag the system for remediation.

If the system is found to not contain attributes or open vulnerabilities, the analyst will select a negative result and the IncMan incident will be updated with the vulnerability findings and close the incident.

TENABLE.IO ACTIONS

Enrichment

- Create Scan
- Execute Scan
- Get Scan CSV Report
- List Templates
- Scan and Get Report

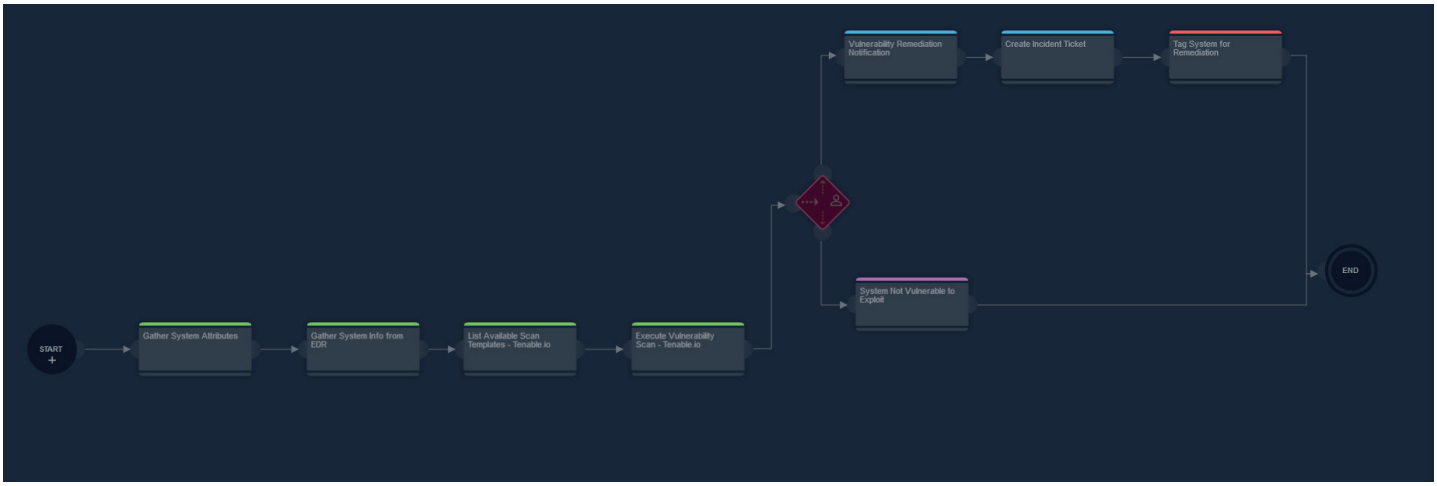

Fig 1. R^3 Runbook

Automate.
Orchestrate.
Measure.

About DFLabs.

DFLabs is an award-winning and recognized global leader in Security Orchestration, Automation and Response (SOAR) technology.

Its pioneering purpose-built platform, IncMan SOAR, is designed to manage, measure and orchestrate security operations tasks, including security incident qualification, triage and escalation, threat hunting & investigation and threat containment. IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of security operations teams, reducing the time from breach discovery to resolution and increasing the return on investment for existing security technologies.

As its flagship product, IncMan SOAR has been adopted by Fortune 500 and Global 2000 organizations worldwide. The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121.

DFLabs has operations in Europe, North America and EMEA.

For more information visit www.dflabs.com or connect with us on Twitter @DFLabs.

CONTACT US

US – +1 201 579 0893
UK – +44 203 286 4193
IT – +39 037 382 416

E – sales@dflabs.com

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.

DFLABS.COM

Automate.
Orchestrate.
Measure.

tenable® | DFLABS CYBER INCIDENTS UNDER CONTROL