INTERGRATION BRIEF

Cisco Threat Grid and DFLabs.

Accelerate Incident Investigations with Cisco and DFLabs

Automate.
Orchestrate.
Measure.

CISCO | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

The partnership between DFLabs and Cisco Threat Grid helps organizations effectively defend against both targeted attacks and threats from advanced malware by providing a unified malware analysis and context-rich intelligence tool in one solution.

In addition to this unified solution, Cisco Threat Grid provides a safe environment to dissect malware without the risk of infecting an organization's network.

Analysts of all levels can interact with a malware sample using proprietary and highly secure static and dynamic analysis techniques. Correlation of the results are based on behavioral indicators derived from the historical and global context of hundreds of millions of other analyzed malware artifacts to provide a comprehensive view of malware attacks, campaigns, and their distribution.

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

The Problem.

Adversaries and their methods are constantly evolving which has caused the industry to create more advanced tools to combat their efforts. These advanced tools are often segregated causing analysts to waste valuable time navigating through their toolsets before they can even begin to construct the incident's details.

Once the evidence is collected, full analysis may be restricted for those who do not have the means to deploy a safe testing and analysis environment to assess the capabilities of potentially malicious files. To make matters worse, the industry is lacking qualified individuals to perform the advanced analysis of these malicious files necessary to prevent a possible breach. The combination of these shortcomings has created a perfect storm of obstacles network defenders and incident responders must overcome.

CHALLENGES

- How can orgainzations automate the manual process of information gathering?
- Information gathering tedious manual process
- Valuable time wasted navigating multiple tools to provide necessary malware analysis and threat detection
- How can organizations regain the valuable time wasted navigating multiple toolset required to perform the crucial task of malware analysis and threat detection?
- Lack of qualified individuals to perform necessary analysis
- How can organizations overcome the lack of qualified candidates necessary for full and complete analysis of threats?

The DFLabs and Cisco Threat Grid Solution.

The DFLabs and Cisco solution extends these industry-leading capabilities by automating intelligence gathered from Threat Grid's comprehensive toolset, investigators can be presented with the evidence necessary to prioritize an incident and quickly act to minimize the time an attacker has to dwell in an environment.

Automate.
Orchestrate.
Measure.

About Cisco Threat Grid.

Cisco Threat Grid combines static and dynamic malware analysis with threat intelligence into a single solution delivered through the cloud, as an on-premises solution, or integrated into Cisco security technologies. Threat Grid combines behavioral analysis and up-to-the-minute threat intelligence feeds with your existing security infrastructure. With Threat Grid you can

understand what malware is doing or attempting to do, how large a threat it poses, and how to defend against it.

About DFLabs 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.

A user reports that they opened a file which was sent to them from who they believed to be a known source. After opening the file, the user started to notice extreme lag and their computer continues to crash and display strange behavior. The user sends the suspicious file and all associated information using an engagement form.

Upon receipt of the form, IncMan automatically begins to process the artifacts included in the form by detonating the suspicious file with Cisco Threat Grid and running reputation checks through multiple sources. Once this initial information gathering is performed, IncMan comes to its first conditional argument. If the file's threat score reported by Threat Grid is greater than 50, IncMan automatically blocks the IP address at the firewall and queries Threat Grid to gather PCAP information from during the timeframe the file was received.

IncMan will pass the file's hash value to the EDR solution to search for additional hosts who may have received the malicious file. If the EDR solution finds that additional hosts have received the file, IncMan will simultaneously prompt the EDR solution to quarantine the reporting host and ban the hash, add the additional hosts to the incident and upgrade the priority to critical, create an incident ticket in the company's ticketing system and send a notification email to the responsible party for further review and remediation actions.

CISCO THREAT GRID ACTIONS

Enrichment

- URL Reputation
- IP Reputation
- Domain Reputation
- Detonate File
- Detonation Report
- Detonate URL
- PCAP of a Detonated File

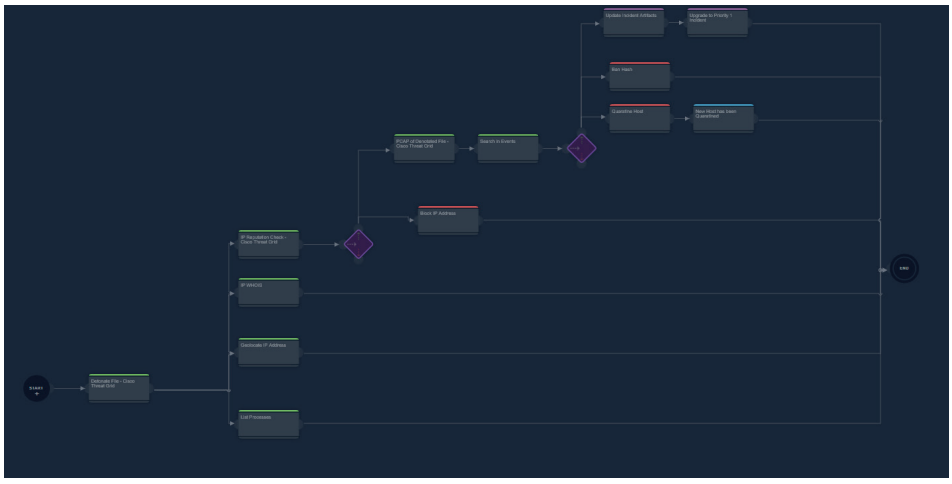

Fig 1. R^3 Runbook

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

Cisco Threat.

Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

For more information visit www.cisco.com/c/en/us/products/security/threat-grid/index.html

DFLABS.COM

Automate.
Orchestrate.
Measure.

CISCO | DFLABS CYBER INCIDENTS UNDER CONTROL