INTEGRATION BRIEF

DFLabs and Cuckoo Sandbox:

Automate Advanced Dynamic Malware Analysis.

Automate the advanced dynamic analysis of malware using the power of Cuckoo Sandbox.

DFLABS.COM

Automate.
Orchestrate.
Measure.

cuckoo | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Malware has become increasingly complex and difficult to examine. To fully understand the capabilities of many malware samples, advanced analysis is required; something which can be both time consuming and require a unique skillset. DFLabs IncMan SOAR's integration with Cuckoo Sandbox allows users to automate the dynamic analysis of malicious and unknown files, providing critical information during the incident response process. Cuckoo Sandbox provides critical insights in to the capabilities of a file, providing the basis for additional automated and manual decisions on the appropriate response to an incident.

Automate the dynamic analysis of malicious and unknown files, providing critical information during the incident response process.

The Problem.

Malware has become increasingly complex and difficult to examine. The rate at which new malware is released, combined with the detection evasion techniques employed by modern malware means that traditional anti-malware solutions and scanning techniques are sometimes ineffective. In cases where other detection and analysis tools are ineffective, or more detailed information about the malware is required, a more in-depth analysis solution is needed.

DFLABS.COM

The DFLabs and Cuckoo Solution.

DFLabs IncMan SOAR's integration with Cuckoo Sandbox allows users to automate the dynamic analysis of malicious and unknown files, providing critical information during the incident response process.

Using Cuckoo Sandbox's open source and highly customizable dynamic malware analysis capabilities, organizations can automate the advanced analysis of malicious and unknown files as part of the automated and orchestrated response to a potential security incident. Cuckoo Sandbox provides critical insights in to the capabilities of a file, providing the basis for additional automated and manual decisions on the appropriate response to an incident.

DFLabs IncMan SOAR and Cuckoo Sandbox solve these specific challenges:

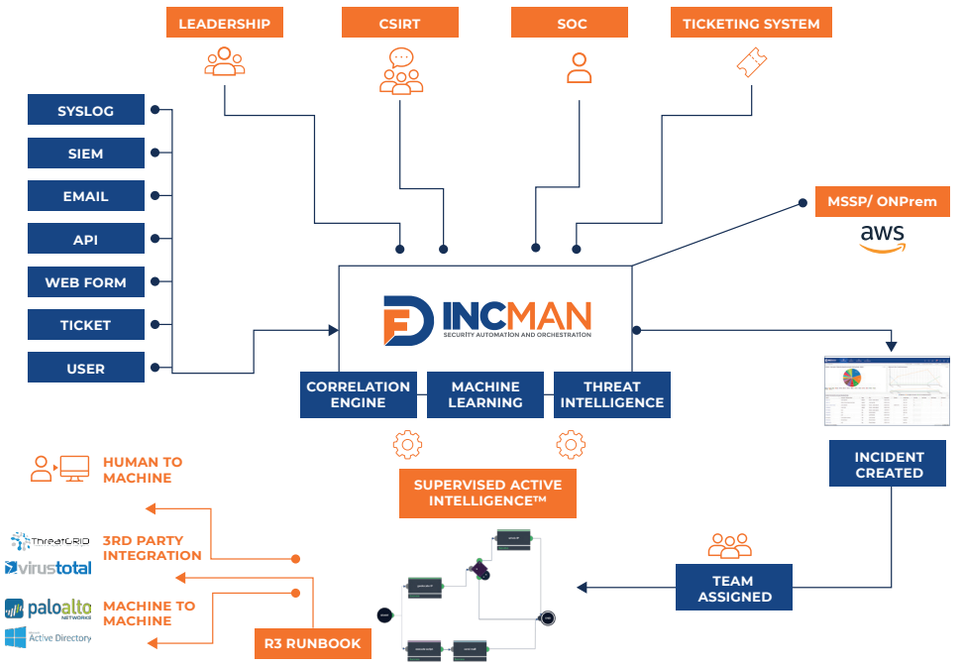
- How can I perform advanced analysis of unknown files?
- How can I determine the potential capabilities of malicious files?
- How can I quickly extract indicators from a malicious file?

Combining IncMan SOAR, Cuckoo Sandbox and other security products enables Enterprises to:

- Reduce incident resolution time by 90%
- Maximize security analyst efficiency by 80%
- Increase the number of handled incidents by 300%

Automate.
Orchestrate.
Measure.

DFLabs IncMan SOAR Overview.



About Cuckoo.

Cuckoo Sandbox is the leading open source automated malware analysis system. You can throw any suspicious file at it and in a matter of minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment.

Malware is the swiss-army knife of cybercriminals and any other adversary to your corporation or organization.

In these evolving times, detecting and removing malware artifacts is not enough: it's vitally important to understand how they operate in order to understand the context, the motivations, and the goals of a breach.

Cuckoo Sandbox is free software that automated the task of analyzing any malicious file under Windows, OS X, Linux, and Android.

About DFLabs IncMan SOAR.

DFLabs IncMan Security Orchestration, Automation and Response (SOAR) platform automates, orchestrates and measures security operations and incident response tasks, including threat validation, triage and escalation, context enrichment and threat containment.

IncMan SOAR uses machine learning and Rapid Response Runbooks (R^3 Runbooks) as a force multiplier that has enabled security teams to reduce average incident resolution times by 90% and increase incident handling by 300%.

CHALLENGES

- How can I perform advanced analysis of unknown files?
- How can I determine the potential capabilities of malicious files?
- How can I quickly extract indicators from a malicious file?

DFLABS AND CUCKOO SOLUTION

- Perform advanced analysis to determine capabilities of unknown files
- Extract indicators from malware
- Search for additional indicators of compromise on the network
- Block indicators to prevent further compromise

RESULTS

- Reduce Incident resolution time by 90%
- Maximize security analyst efficiency by 80%
- Increase the number of resolved incidents by 300%

Automate.
Orchestrate.
Measure.

Use Case.

The following Runbook could have many potential applications, from examining a suspicious email attachment to an unknown executable found on a host.

The Runbook begins by submitting the file to Cuckoo for analysis. IncMan SOAR allows the user to select the virtual machine which will be used to execute the file, which can be set as a default or chosen by the user at runtime.

Following the Cuckoo execution, the Runbook retrieves the analysis from Cuckoo. As part of the analysis, Cuckoo extracts and documents many artifacts which can be further enriched, including network connection attempts, embedded URLs, dropped files and files gathered from process memory.

The Runbook continues by submitting these artifacts through the appropriate reputation services. Following these reputation queries, a search of the organization's SIEM or EDR solution is performed for any artifacts which were deemed potentially malicious. If the organization's SIEM or EDR solution returns any results, indicating that the potentially malicious artifact has been observed in the organization's environment, a notification is sent to the appropriate parties to initiate further investigation.

This Runbook demonstrates how easily it is to automatically pivot from a simple Cuckoo analysis report to quickly check the organization's environment for additional evidence of malicious activity.

This Runbook could easily be expanded to include automated or semi-automated containment actions, as well as other enrichment actions.

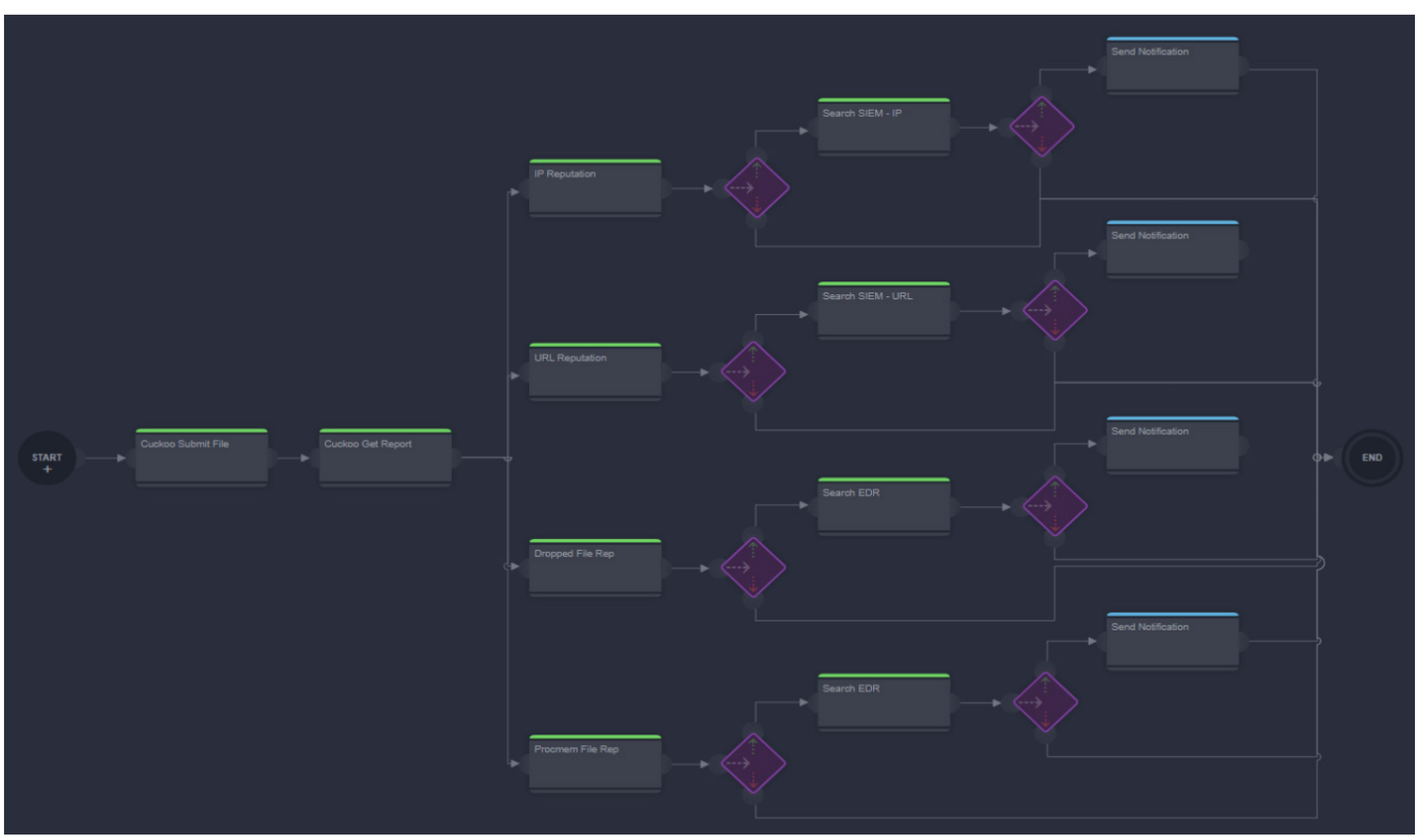
RECORDED FUTURE ACTIONS

Enrichment

- Detonate File
- Detonate URL
- Detonation Report

LEARN MORE

For more information on how to take your incident response to the next level with DFLabs IncMan SOAR, contact your DFLabs representative or visit www.dflabs.com.



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 – +39 037 832 416

E – sales@dflabs.com

About Cuckoo.

Cuckoo Sandbox is the leading open source automated malware analysis system. You can throw any suspicious file at it and in a matter of minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment.

Malware is the swiss-army knife of cybercriminals and any other adversary to your corporation or organization.

In these evolving times, detecting and removing malware artifacts is not enough: it's vitally important to understand how they operate in order to understand the context, the motivations, and the goals of a breach.

Cuckoo Sandbox is free software that automated the task of analyzing any malicious file under Windows, OS X, Linux, and Android.

Learn more at www.cuckoosandbox.org and follow us on Twitter at @cuckoosandbox.

Automate.
Orchestrate.
Measure.