INTERGRATION BRIEF

Cisco Umbrella and DFLabs.

Protecting Users from Anywhere with DFLabs and Cisco Umbrella

Automate.
Orchestrate.
Measure.

CISCO | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

The partnership between Cisco Umbrella and DFLabs gives organizations' the ability to extend their protection strategies beyond their internal network by providing a first line of defense for users anywhere their responsibilities may take them. Whether on or off an organizations' network, Cisco Umbrella blocks malicious threats before they reach their users and provides network defenders greater visibility and protection capabilities Internet-wide.

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

The Problem.

Organization's users are becoming more mobile as the world becomes more digitally interconnected. This shift from purely on-prem defense strategies to a complicated mix between traditional defenses and the need to extend beyond our common boundaries has created a difficult dilemma for network defenders. As more users and infrastructures are migrating to the cloud and Internet threats become more sophisticated, the need for greater visibility, intelligence, protection, and rapid response has left the industry scrambling to keep up.

CHALLENGES

- How can organizations secure their workforce operating outside of an organization's perimeter?
- More users are operating outside of an organization's perimeter
- Traditional security efforts are no longer adequate
- How can organizations upgrade traditional security practices to combat today's sophisticated threats?
- Need for complete visibility has become more difficult as applications and users are migrated to the cloud
- How can organizations gain complete visibility into their environments as more applications and users migrate to the cloud?

The DFLabs and Cisco Umbrella Solution.

The DFLabs and Cisco solution takes Umbrella's protection, intelligence and visibility capabilities and extends them to an organization's integrated technologies. This ability to extend these protections provides not only the advanced capabilities needed to protect our networks on the go but allows for rapid response efforts to the sophisticated threats today's environments and its users are facing.

Automate.
Orchestrate.
Measure.

About Cisco Umbrella.

Cisco Umbrella is a cloud security platform built into the foundation of the internet. Enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established — stopping threats over any port or protocol before they reach your network or endpoints.

As a cloud-delivered service, Umbrella provides the visibility needed to protect internet access across all network devices, office locations, and roaming users. All internet activity is logged and categorized by the type of security threat or web content, and the action taken — whether it was blocked or allowed. Logs of all activity can be retained as long as needed and recalled easily for investigation. Organizations can even uncover cloud apps and Internet of Things (IoT) devices in use across their environment.

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.

An IDS alert for a potentially malicious redirect is received after a user visits a suspicious URL. IncMan simultaneously begins to query Cisco Umbrella Investigate for WHOIS information regarding the domain visited, as well as performing a DNS lookup on the domain to gather more information on the actor. The domain and IP address are then fed into Umbrella's reputation checking system and the EDR solution is queried for additional hosts which may have visited the site in the past.

Once the initial information gathering is completed, IncMan comes to its first set of conditional statements. The first conditional statement makes a decision on what action should be taken next if the observed domain is found to be malicious. If it reports a threat score above 50, a user choice action is presented. This will allow an analyst or network defender to review the information gathered and make a decision whether to take containment actions through Cisco Umbrella to block the domain from the network.

The second conditional statement determines if any other host on the network has been observed in communication with this malicious IP or domain. If it is found that more than the initial host has communicated with the malicious actor, the additional artifacts will be added to the incident and another user choice condition is presented. This user choice prompts the analyst or network defender to review the information gathered and to decide whether more than one host should be quarantined and added to the incident.

If no additional hosts have been identified, IncMan will automatically update the incident with the additional artifacts gathered during the investigation and quarantine the affected host, block the IP address, and ban the hash from the network. Once the automation tasks have completed, IncMan will create a new ticket within the organization's ticketing system and send out notification of the incident.

CISCO UMBRELLA ACTIONS

Enrichment

- Domain Reputation
- IP Reputation
- Domain WHOIS
- Email WHOIS

Containment

- Block Domain
- Unblock Domain

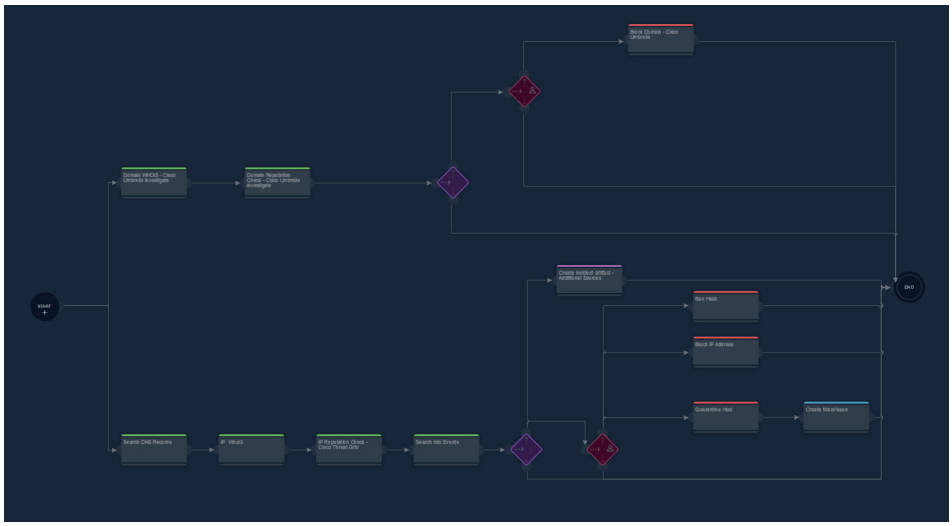

Fig 1. R³ Runbook

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 Cisco Umbrella.

Cisco Umbrella is a cloud-delivered security service that brings together essential functions that you can adopt incrementally, at your pace. Umbrella unifies secure web gateway, DNS-layer security, cloud-delivered firewall, cloud access security broker functionality, and threat intelligence.

For more information visit www.umbrella.cisco.com/

DFLABS.COM

Automate.
Orchestrate.
Measure.

CISCO | DFLABS CYBER INCIDENTS UNDER CONTROL