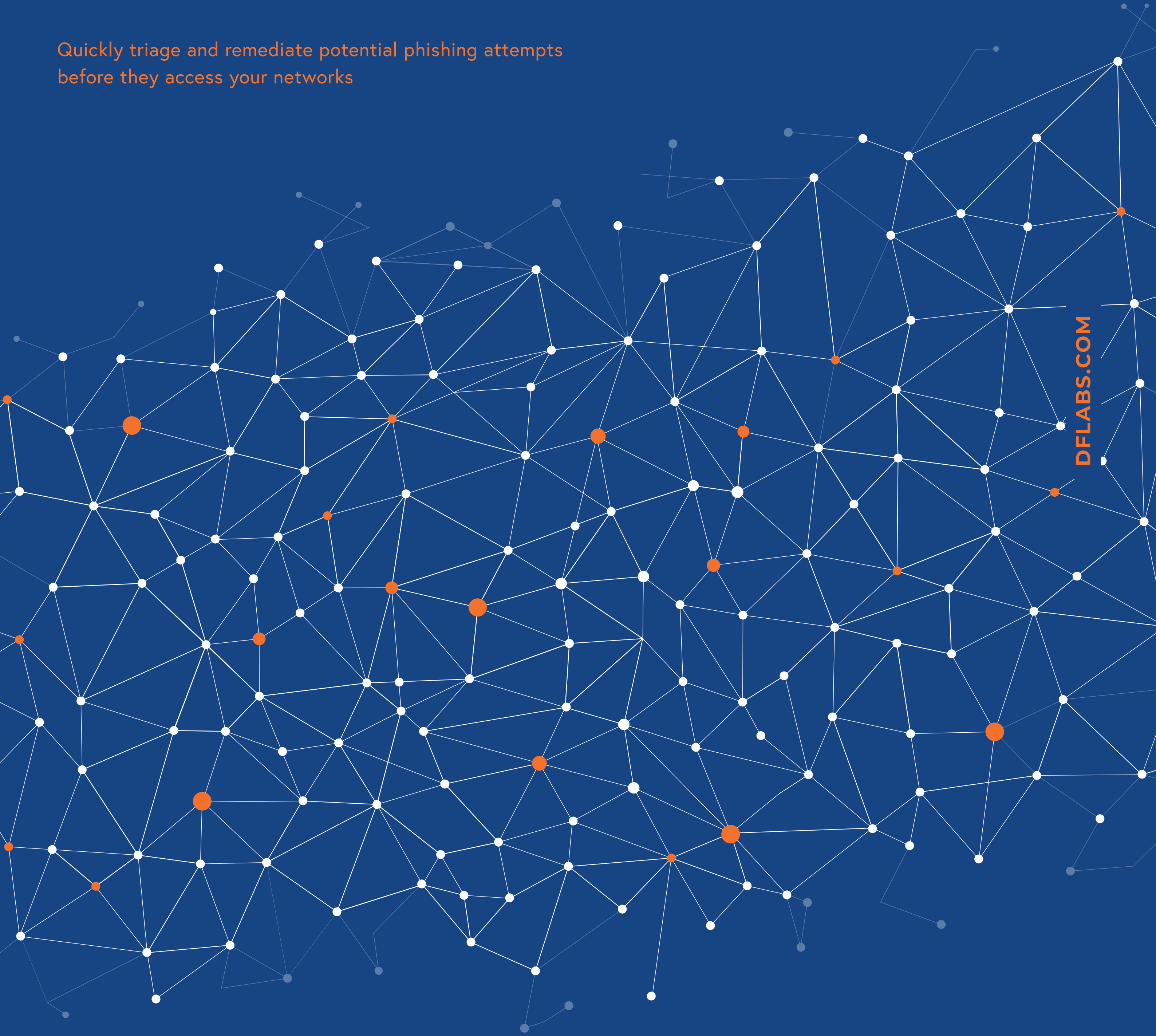
INTERGRATION BRIEF

# Rapidly Detect and Respond to Phishing Attacks with Cofense and DFLabs.

Quickly triage and remediate potential phishing attempts before they access your networks



DFLABS.COM

Automate.
Orchestrate.
Measure.

COFENSE | DFLABS CYBER INCIDENTS UNDER CONTROL

## Solution Overview.

Having the ability to quickly triage a potential phishing scam gives an incident responder the edge they need to stay ahead of their adversaries. However, determining whether the intent of the message is benign or malicious takes a lot of manual investigation which wastes valuable time.

DFLabs' integration with Cofense provides the answer incident response teams have been looking for by combining Cofense's powerful phishing-based threat intelligence with IncMan SOAR's automation capabilities to quickly triage and respond to a potential scam before the attacker has the ability to take up residence in an environment. Armed with the intelligence necessary to spot a threat, incident responders can shut down an attacker's campaign in seconds rather than the hundreds of days they are currently lying dormant in breached environments.

- Quickly detecting and prioritizing a phishing attempt gives incident responders a head-start in containing a potential incident
- Thwarting an attacker's ability to utilize stolen credentials prevents an incident from turning into a full-blown breach
- Removing the manual triaging process allows incident responders to quickly contain a potential attacker before they have a chance to pivot and wreak havoc on an environment

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

## The Problem.

As with all cyberattacks, phishing attacks are growing in sophistication each year. One of the largest threats associated with these types of attacks is the spread of malware throughout an organization. However, the industry is beginning to see a shift in this trend from deployment of malware to credential theft.

This shift is due to the attack vector's high success rates and an attacker's ability to gain unfettered access to elevate privileges and move about the network freely without detection. An attacker's ability to lie undetected is contributed to by ineffective detection capabilities and responder's extended resolution times. Detecting and investigating phishing attacks continue to be a daunting manual process which causes valuable time to be wasted and prevents responders from quickly containing an attacker once access is gained.

### CHALLENGES

- How can incident responders defend against phishing and social engineering attacks which continue to become more sophisticated?
- How can network defenders prevent credential theft in their environments?
- How can the triaging process become more streamlined?

## The DFLabs and Cofense Solution.

The DFLabs and Cofense solution brings rapid response to phishing campaigns by providing incident responders with rich intelligence the moment a suspected malicious email is received. Coupled with the automation power of IncMan's Rapid Response (R3) Runbooks, these malicious attacks can be triaged, compared to historical data, re-prioritized and contained all before a responder is even alerted to a potential incident.

This type of rapid response is the only defense responders have to these extremely sophisticated types of attacks. As the sophistication grows and the success rates rise, this attack type will continue to be the go-to for an adversary and organizations need to be prepared. By utilizing DFLabs and Cofense's integration, incident response teams can rest assured that they are ready.

**Automate.**
**Orchestrate.**
**Measure.**

## About Cofense.

Cofense combines market-leading incident-response technologies with employee-sourced attack intelligence for a complete collective defense against email-based cyberattacks. Cofense focuses on solutions for the problem of phishing – the most effective attack vector used in more than 90% of successful breaches.

Cofense is dedicated to providing the highest quality cyber security solutions and continue to innovate with dozens of patented technologies used in their solutions. Cofense has been recognized as an industry leader with awards including Deloitt's Technology Fast 500, INC 5000, SC Magazine's BEST Awards, E&Y, and Tech Trailblazers to name but a few.

## 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.

IncMan SOAR receives a potential phishing email forwarded to the security team by a user suspicious of the email's content. Upon receipt of the message, IncMan automatically begins to gather information on the email message, any of its attachments, and its sender from Cofense's threat intelligence platform.

The email's threat report is downloaded and added to the incident as an artifact and IncMan comes to its first decision point in the incident's R3 Runbook. This conditional action looks for negative reputation scores for either the sender's domain or the email's attachment. If either of those components report a negative reputation, IncMan will search through the organization's mail server to see if anyone else in the company had received the same attachment or an email from the sender. Once the additional mailboxes are evaluated, the R3 Runbook comes to its second conditional statement. This statement is looking for the presence of any additional user having received an email communication from the sender or the same reported attachment. If an additional user has met the condition, the user's details are extracted from the organization's directory services and added to the incident as an artifact.

The user's information is then fed into the company's SIEM to query for any additional security events originating from their account. If the account had been observed in another security incident, the R3 Runbook automatically upgrades the incident to a critical priority and begins to disable the user, reset their password, and creates trouble ticket for the IT helpdesk to assist the user with their disabled account and issue a critical priority incident ticket for the company's incident response team.

If the user's account has not been involved in any additional security alerts, IncMan will upgrade the incident's priority to high and follow the same execution path to reset the user's password and involve both the IT helpdesk and the incident response team.

If no additional users have been observed in communication with the sender or have received the potentially malicious attachment, the R3 Runbook initially sets the incident's priority to medium and gathers the original auditing team member's details from their directory services. This information is then fed through the SIEM to see if their account had been involved in any additional security alerts. If the account has been involved in an additional security alert, the priority is adjusted to high and follows the high priority incident execution path. If the account has not been observed in any additional security alerts, a medium priority ticket is issued for the incident response team to further investigate the phishing activity.

### COFENSE ACTIONS

**Enrichment**

✓ Get Report

✓ Threat Search

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 Cofense.

Cofense combines market-leading incident-response technologies with employee-sourced attack intelligence for a complete collective defense against email-based cyberattacks. Cofense focuses on solutions for the problem of phishing – the most effective attack vector used in more than 90% of successful breaches. from the Cb Predictive Security Cloud, Cb Protection ensures that only trusted and approved software is allowed to execute an organization's critical systems and endpoints.

For more information visit www.cofense.com

DFLABS.COM

Automate.
Orchestrate.
Measure.

COFENSE

DFLABS
CYBER INCIDENTS UNDER CONTROL