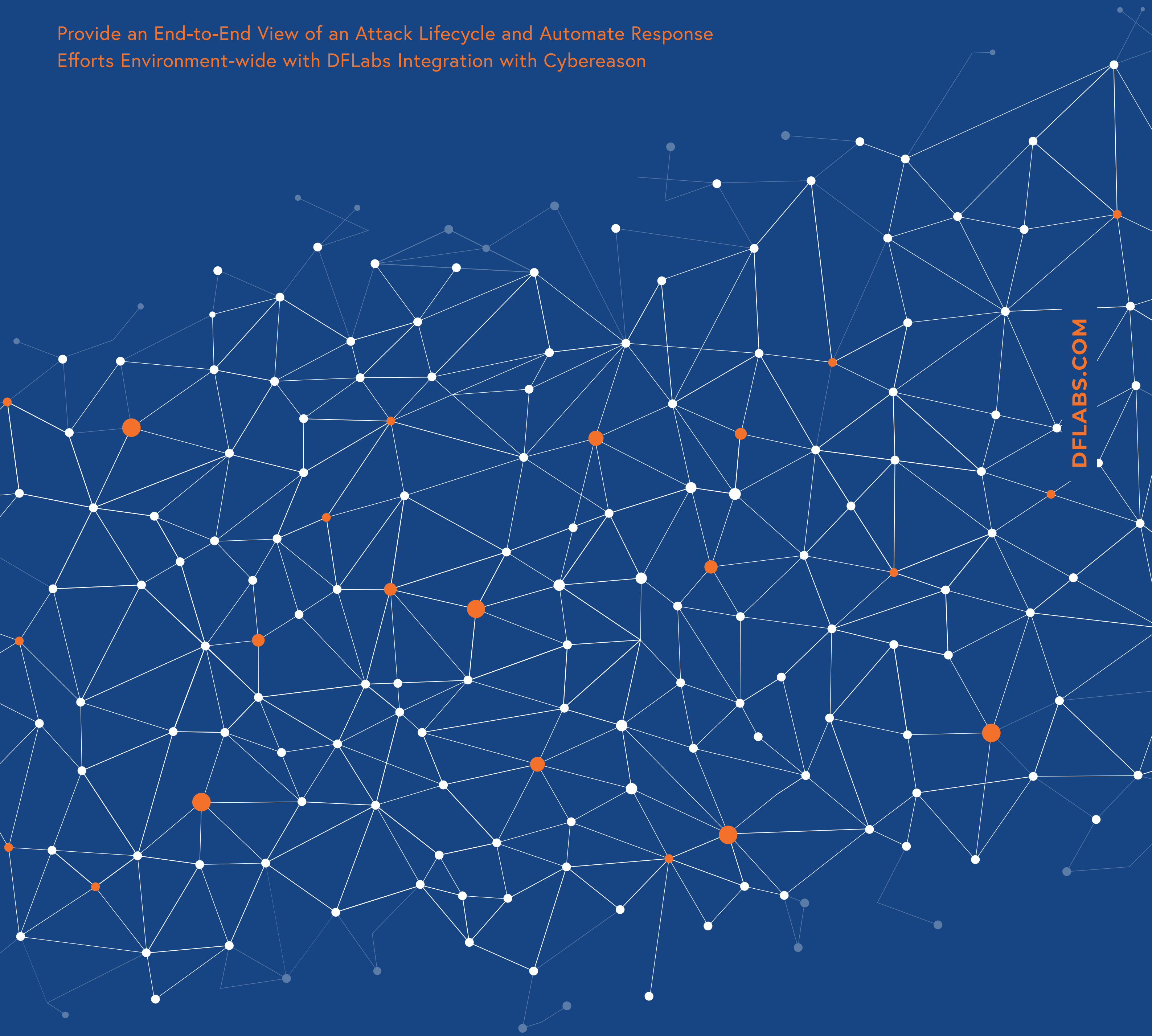
INTERGRATION BRIEF

Improve the Remediation Process and Empower Security Professionals with DFLabs and Cybereason.

Provide an End-to-End View of an Attack Lifecycle and Automate Response Efforts Environment-wide with DFLabs Integration with Cybereason



DFLABS.COM

Automate.
Orchestrate.
Measure.

cybereason

DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Providing context into the entire attack lifecycle and the ability to take automated action to remediate an incident through DFLabs integration with Cybereason gives organizations a leg up on a would-be attacker.

Through the use of Cybereason's industry-leading Endpoint Detection and Response (EDR) platform, network defenders can quickly identify potential endpoint incidents and perform a complete root cause analysis to find the source of malicious activity. Armed with this context, automated actions can be taken instantly to contain a threat before it has a chance to spread laterally through a network.

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

The Problem.

One of the biggest problems, besides qualified staffing and alert fatigue, Security Operation Centers experience is a lack of context behind alerts being received. More and more organizations are subscribing to threat intelligence feeds and purchasing the latest product lines only to be overwhelmed with information without context or a clear path towards remediation.

The lack of context and remediation has led to dwell times measuring in the hundreds of days, which is allowing attackers more time to remain undetected and cause significant damage. Without context and immediate action to remediate the activity, an avoidable incident can escalate to a full-blown breach.

CHALLENGES

- Dwell times are being measured in the hundreds of days
- Numerous disperse security and network technologies are causing organizations to lack the complete visibility needed to see the entirely lifecycle of an attack
- Lack of context is making threat detection and remediation capabilities more difficult for network defenders

DFLabs and Cybereason Solution.

DFLabs integration with Cybereason enhances the identification and remediation of incidents by combining context-rich visibility into an attack with complete orchestration capabilities in which to utilize all products within an organization's security stack. This combination will also allow security and IT teams to work in concert with each other by providing the context necessary to convey an issue, regardless of the level of security knowledge, to make joint decisions quickly to reduce the impact of an incident. Finally, this integration also has the added benefit of allowingsecurity teams to present this risk data to executive management in a clear and effective way.

- Greater context into alerting for better prioritization and remediation of incidents
- Full network visibility and containment capabilities in order to effectively utilize an organization's entire security stack
- Reduction of dwell times by accessing data on an entire attack lifecycle to determine the source of an infection

Automate.
Orchestrate.
Measure.

About Cybereason.

The Cybereason real-time attack detection and response platform brings military-grade defense to enterprises, providing automated detection, complete situational awareness and a deep understanding of attacker activities.

Cybereason automatically detects malicious activity and presents it in an intuitive way, provides end-to-end context of an attack campaign and deploys easily with minimal organizational impact. Organizations are able to deploy and can start detecting within 24-48 hours.

With continuous 24/7 monitoring, Cybereason provides complete situational awareness across an entire IT environment, allowing organizations respond to incidents quickly and efficiently.

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 alert is received from Cybereason's Detection and Response Platform indicating that a suspicious executable (.exe) has been observed on several hosts in the Payroll Department. IncMan receives the alert and begins to retrieve detonation information for the suspicious program.

Once this information has been collected, IncMan queries Cybereason for the items reputation score. Based off the findings of the detonation and reputation checks, IncMan will come to its first decision point. If the detonation verdict finds the program to be malicious, IncMan will automatically block the application across the network and begin querying the organization's SIEM for all hosts who received the .exe file.

Upon identifying the affected machines, IncMan will update the current incident with these additional hosts and create an isolation rule in Cybereason to isolate them from the network. Once the hosts have been isolated, IncMan will create a new incident ticket in the organization's ticketing system to alert the Operations Team of the potential incident and isolation of hosts.

CYBEREASON ACTIONS

Enrichment

- Get Isolation Rules
- Get Items Reputation
- List Endpoints

Containment

- Create Isolation Rule
- Update Isolation Rule
- Delete Isolation Rule
- Set Item Reputation

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 Cybereason.

The Cybereason real-time attack detection and response platform brings military-grade defense to enterprises, providing automated detection, complete situational awareness and a deep understanding of attacker activities.

Cybereason automatically detects malicious activity and presents it in an intuitive way, provides end-to-end context of an attack campaign and deploys easily with minimal organizational impact.

Organizations are able to deploy and can start detecting within 24-48 hours.

For more information visit www.cybereason.com

DFLABS.COM

Automate.
Orchestrate.
Measure.

cybereason

DFLABS
CYBER INCIDENTS UNDER CONTROL