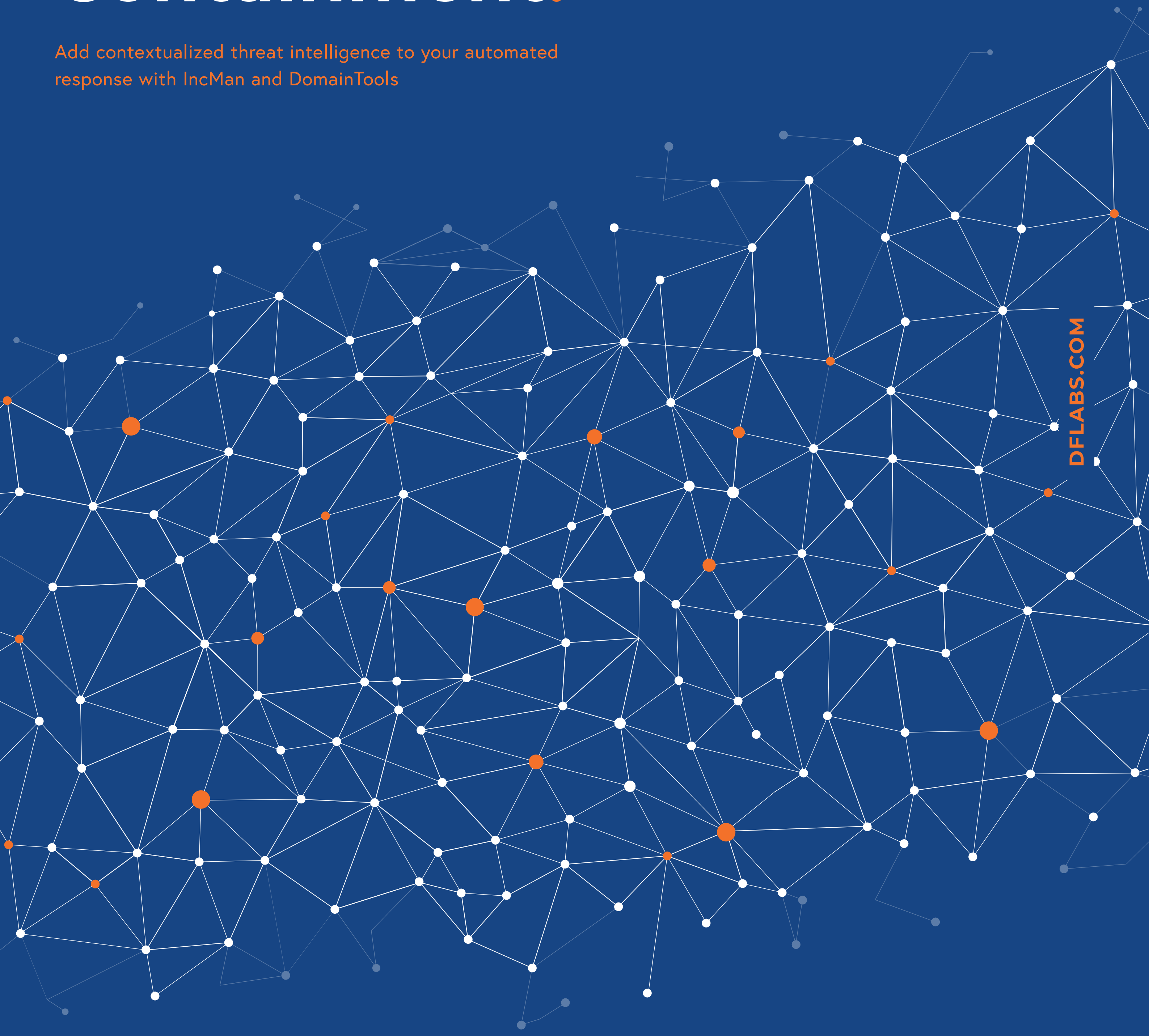
INTERGRATION BRIEF

Combining Real-Time Threat Data with Powerful Automated Containment.

Add contextualized threat intelligence to your automated response with IncMan and DomainTools



DFLABS.COM

Automate.
Orchestrate.
Measure.

DOMAINTOOLS

DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

The ability to quickly gather actionable threat intelligence gives an organization the vital information needed to make informed decisions early on in the incident response process. With human error still being one of the top intrusion tactics, the odds of an organization experiencing a breach is no longer a matter of if, but a matter of when.

DFLabs' integration with DomainTools is focused on empowering network defenders by automatically gathering actionable threat intelligence from one of the industry's leading platforms to quickly prioritize and contain would-be attackers. DFLabs and DomainTools arms security analysts with real-time intelligence and automated containment capabilities to lessen the chance of an intruder accomplishing their goals and causing irreparable damage to an organization's operations and reputation.

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

The Problem.

Phishing campaigns are one of the most successful means of an initial intrusion into a networked environment. Even with tireless user training somehow these adversaries still find a way to deceive users into falling for their tactics.

Since human error is hard to predict and defend against, security professionals need to be able to detect and remediate a user's lapse in judgement. Without the ability to detect and quickly respond to phishing-based attacks, organizations run the risk of having intruders lying in wait until their goals has been achieved and the damage has been done.

CHALLENGES

- Phishing continues to be the most successful intrusion tactic
- Human error is extremely hard to predict and defend against
- If a phishing intrusion is not quickly identified and remediated, attackers will linger within a network undetected until the maximum damage is done

DFLabs and Domain Tools Solution.

DFLabs integration with DomainTools provides organizations with the tools necessary for security professionals to quickly identify, prioritize, and remediate potential incidents through the use of real-time threat intelligence and automation power to orchestrate immediate action across an organization's environment.

- Quickly gather incident data to prioritize and respond to a potential incident
- Combat conditions created by social engineering attempts through real-time threat data and containment of suspicious user activity
- Complete orchestration of network and security product to contain incidents before damage can be done to an organization's environment.

Automate.
Orchestrate.
Measure.

About Domain Tools.

DomainTools helps security analysts turn threat data into threat intelligence. They process indicators from an organization's network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

The goal of Domain Tools is to stop security threats to an organization before they happen, using domain/DNS data, predictive analysis, and monitoring of trends on the Internet. By collecting Open Source Intelligence (OSINT) data from many sources, along with historical records, in a central database, Domain Tools index and analyze the data based on various connection algorithms to deliver actionable intelligence, including domain scoring and forensic mapping.

DomainTools has over 10 billion related DNS data points to build a map of 'who's doing what' on the Internet. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work.

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 an organization's SIEM for abnormal activity from a user's email account. A large number of emails were sent from the user's account to multiple recipients in the organization. Upon the receipt of the alert, IncMan automatically begins to gather incident evidence.

The email's domain, IP, and email reputation are checked through DomainTools extensive reputation service. Once these scores have been evaluated, IncMan issues a conditional statement. If either the domain, IP, or email scores a risk reputation of more than 50, IncMan will then query the organization's email service to gather all additional recipients who had received the suspicious email.

Based off the results of the query if any additional users received the email, IncMan issues a request to block the sender and gather the associated attachment from the email. After the sender is blocked and the attachments are gathered, IncMan updates the current incident with the additional victim users and creates an incident ticket within the organization's ticketing system.

While the email is being evaluated, IncMan simultaneously begins to gather information regarding the initial affected user. The organization's directory service is queried to collect the user information and the EDR solution is queried for running processes on the user's system. The system's attributes are gathered and IncMan begins to issue a search for additional events the affected user may have generated. Once this information is gathered, IncMan comes to its second conditional statement. If the SIEM query returns additional events for the affected user, the user's account is automatically disabled, and their password is reset. An email is then sent to both the affected user and the Security team alerting them to the password update and the new incident. Once the troubleshooting ticket is opened and the email notification is sent, the Security team can begin to investigate the incident.

DOMAIN TOOLS ACTIONS

Enrichment

- ✓ Domain Reputation
- ✓ Email Reputation
- ✓ IP Reputation

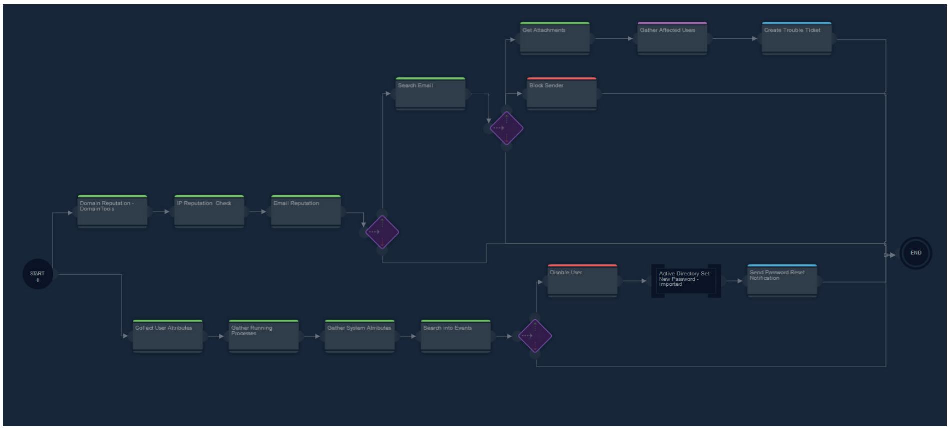


Fig 1. R^3 Runbook

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 Domain Tools.

DomainTools is a leading provider of Whois and other DNS profile data for threat intelligence enrichment. It is a part of the Datacenter Group (DCL Group SA). DomainTools data helps security analysts investigate malicious activity on their networks.

For more information visit www.domaintools.com

DFLABS.COM

Automate.
Orchestrate.
Measure.

DOMAINTOOLS

DFLABS
CYBER INCIDENTS UNDER CONTROL