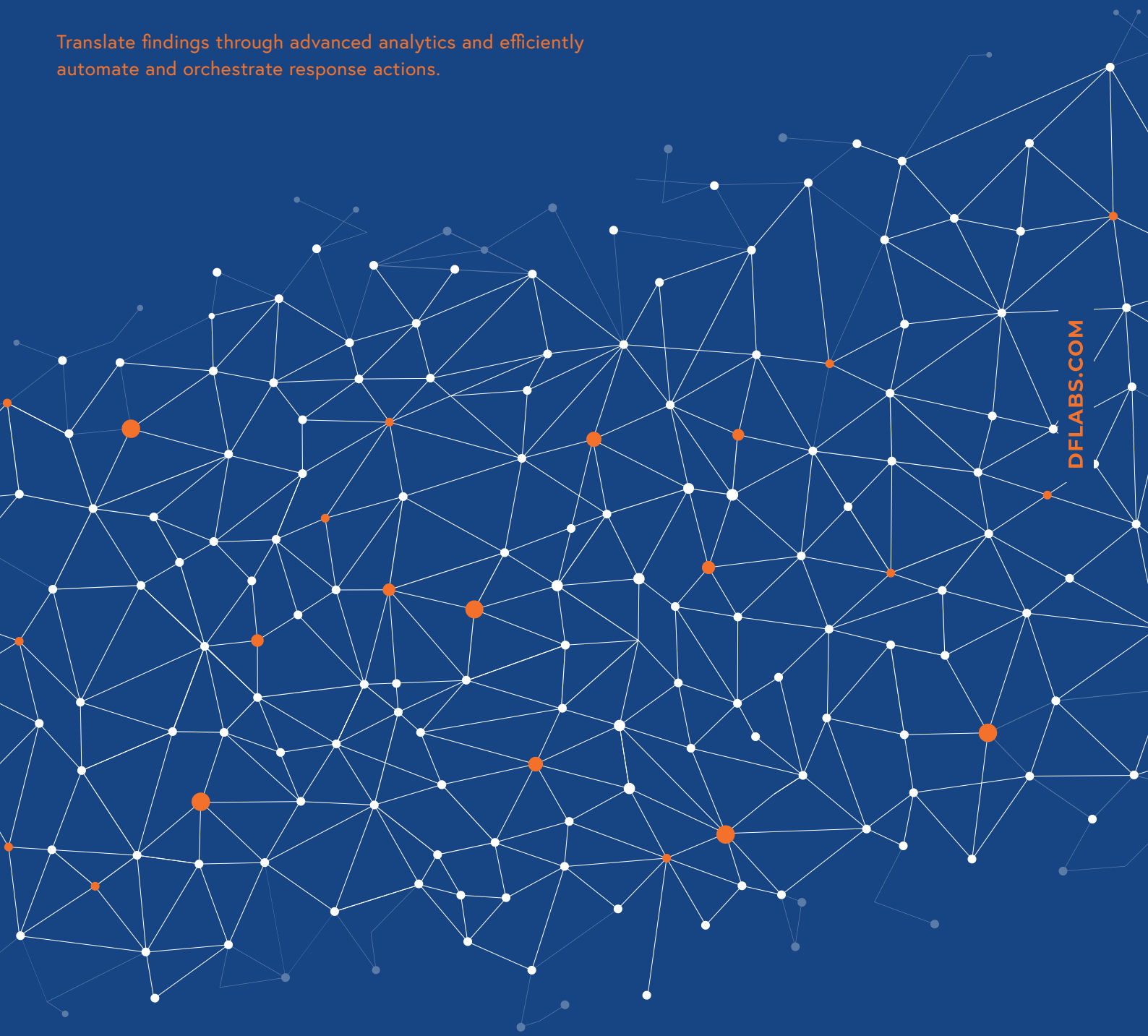
INTERGRATION BRIEF

Achieve Full Visibility and Accelerated Response with DFLabs IncMan SOAR and RSA NetWitness.

Translate findings through advanced analytics and efficiently automate and orchestrate response actions.



Automate.
Orchestrate.
Measure.

RSA | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

To effectively secure and defend modern networked environments an organization must have the ability to not only observe activity across their entire operation, but they also must be able to direct their network and security products to act on their behalf.

DFLabs integration with RSA NetWitness provides organizations with the tools necessary to achieve both full visibility and accelerated response to help fight back against advanced attacks. Through NetWitness' advanced analytics and ability to collect data across multiple capture points, and IncMan's automation power and product orchestration capabilities, this integration will help equip organizations with an added layer of protection against the threats posed towards their businesses.

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

The Problem.

Today's networked environments are more complex than ever before. Between on-prem, public cloud, and hybrid deployments, its no wonder organizations are finding it harder to obtain complete visibility into their environments.

Having this level of visibility is paramount as attackers have evolved their tactics, techniques, and procedures (TTP) to traverse across these modern environments faster than organizations can contain their activities. In order to combat these inefficiencies, organizations are having to also deploy numerous vendor products in an attempt to keep pace with those attackers looking to cause harm.

The necessity to utilize numerous products to provide the protection needed for today's attacks present organizations with another level of complexity. One of the most common struggles organizations are facing is the inability to manage and correlate all of the valuable data across their operations. Each product that provides a layer of protection must be managed individually and cannot always work in concert with other layers of protection. This makes identifying and containing incidents even harder as manual intervention cannot be circumvented.

CHALLENGES

- More complex environments make it hard to obtain complete visibility into networked environments
- Attackers tactics, techniques, and procedures have evolved allowing them to take advantage of the complex nature of today's environments
- Multiple products are necessary to bring advanced detection and remediation capabilities to organizations

DFLabs and RSA NetWitness Solution.

DFLabs integration with RSA NetWitness brings state of the art detection capabilities and the complete visibility necessary for organizations to battle the sophisticated attack techniques that target their operations. Combining these vital toolsets and IncMan's ability to translate their findings into automated actions, the partnership between DFLabs and RSA will act as a force-multiplier for organizations who struggle to find adequate staffing and security protections.

- Provides full visibility into an environment to provide security professionals with a full picture of a potential attack
- Utilization of advanced analytics to uncover advanced attack methods
- Full orchestration and automation capabilities to provide organizations with the added workforce necessary to contain an attacker in real-time before greater damage can be accomplished

Automate.
Orchestrate.
Measure.

About RSA NetWitness.

The RSA NetWitness Platform provides pervasive visibility across a modern IT infrastructure, enabling better and faster detection of security incidents. RSA NetWitness Platform takes security "beyond SIEM," extending the traditional log-centric, compliance-focused approach to security to

include state-of-the-art threat analytics, including user and entity behaviour analytics (UEBA), and visibility into cloud, network and endpoints.

RSA NetWitness Platform solves complex security problems with powerful analytic capabilities. Its modular architecture handles massive amounts of raw data, enriching it with security context at time of capture. It then applies a set of sophisticated analysis tools, including machine learning, UEBA and public as well as RSA community threat intelligence. This process correlates disparate events and alerts into discrete investigations, automatically scoring each according to the likelihood that they represent an attack or exploit.

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.

A Web Application Firewall (WAF) alert is generated for traffic to a potentially compromised web site. IncMan receives the alert and begins to execute automated evidence gathering by querying NetWitness for evidence of this web site being visited by anyone else in the organization. If NetWitness receives a positive hit for any additional browsing activity, IncMan will issue another query to gather the raw logs from all matching activity. While these logs are being gathered, a new ticket is created within the ticketing system and the incident is upgraded to critical.

Simultaneously, the destination IP address and the requested URL's reputation is checked, and the end user's information is queried through directory services and a NetWitness query is issued to gather information on any additional activity observed from the affected user account. Once this information is gathered, IncMan will execute the last two conditional statements. The first statement will look for either the IP address, URL, or detonated URL report to have a risk score of over 50. If a risk score of greater than 50 is reported, IncMan issues a containment action request to the Next-Gen firewall to block both the IP address and URL from further communication.

The last conditional statement looks for additional suspicious activity from the user account. If the user account has been involved in any additional activity, IncMan invokes another runbook to reset the user's password and issue a new randomly generated password, tags the user's machine for further review. Once the password has been reset and the machine is tagged for review, IncMan will issue emails to the affected user and the security team alerting them to the activity and remediation plan.

RSA NETWITNESS ACTIONS

Enrichment

- Retrieve Alert Details
- Retrieve Incident Details
- Search Incidents
- Query
- Retrieve Log Data

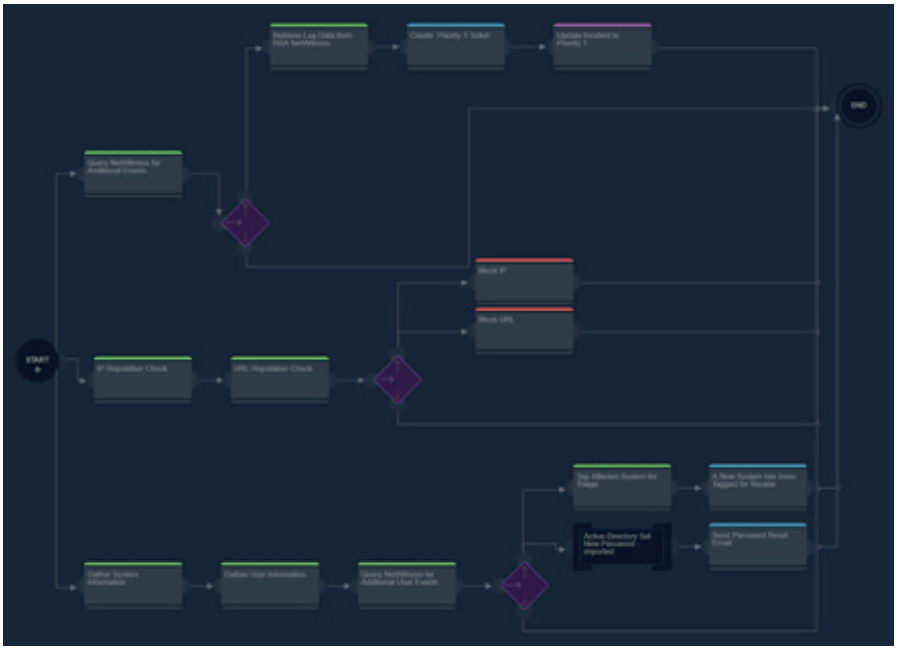


Fig 1. R^3 Runbook

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 RSA NetWitness.

The RSA NetWitness Platform provides pervasive visibility across a modern IT infrastructure, enabling better and faster detection of security incidents. RSA NetWitness Platform takes security "beyond SIEM," extending the traditional log-centric, compliance-focused approach to security to include state-of-the-art threat analytics, including user and entity behaviour analytics (UEBA), and visibility into cloud, network and endpoints.

For more information visit www.rsa.com

DFLABS.COM

Automate.
Orchestrate.
Measure.

RSA | DFLABS
CYBER INCIDENTS UNDER CONTROL