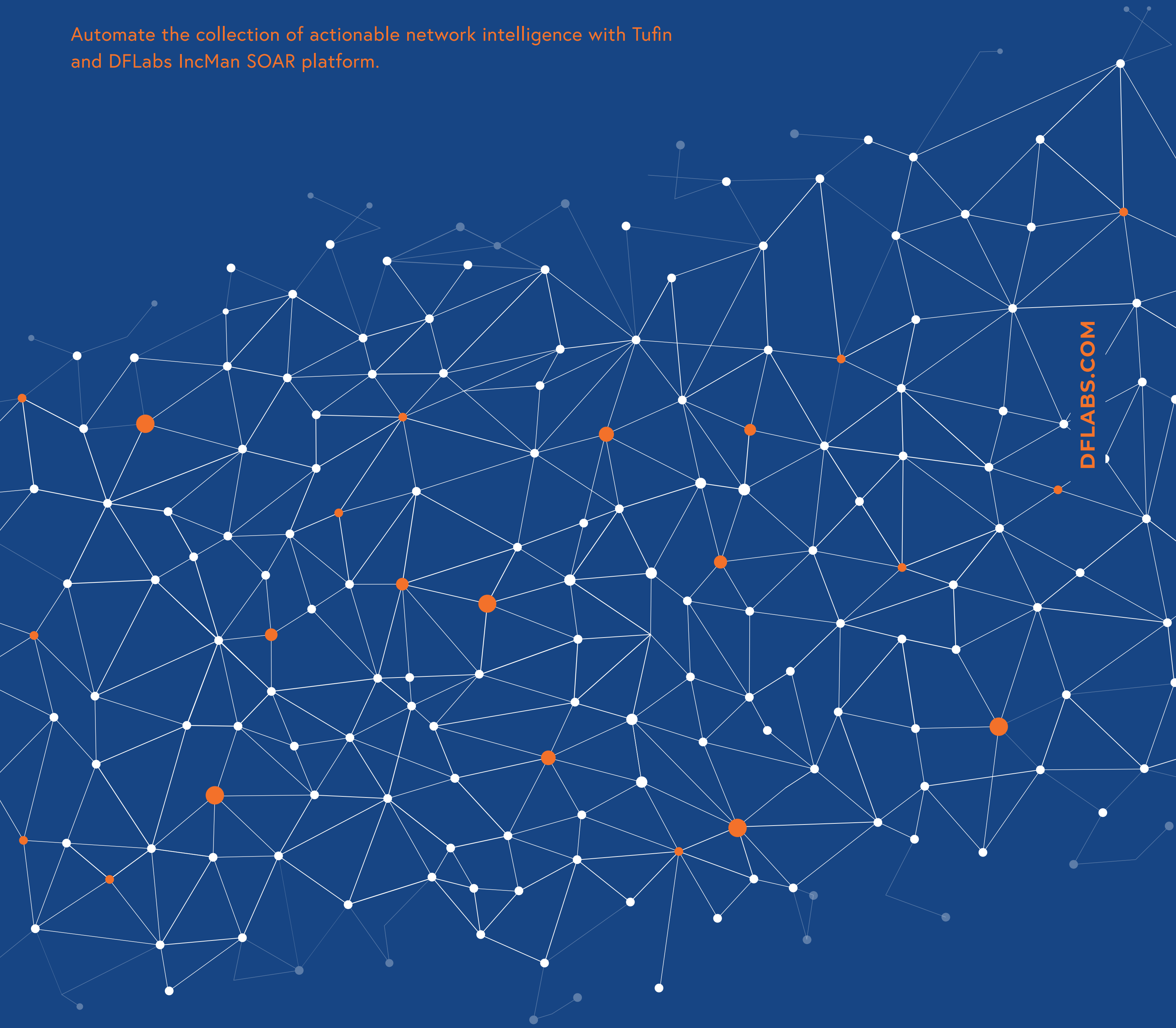
INTEGRATION BRIEF

DFLabs and Tufin: Automate Actionable Network Intelligence.

Automate the collection of actionable network intelligence with Tufin and DFLabs IncMan SOAR platform.



DFLABS.COM

Automate.
Orchestrate.
Measure.

tufin | DFLABS CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Utilize DFLabs IncMan SOAR R3 Rapid Response Runbooks to enable the collection of actionable network intelligence by integrating with Tufin Orchestration Suite.

Harness the vast amount of network intelligence available from Tufin, such as device, policy and path information, along with the automation, orchestration and measurement power of DFLabs IncMan, SOAR to respond faster and more efficiently to computer security incidents.

During an incident it is critical that resonders understand the network topology and have the most current information policy and device information available to them.

The Problem.

Enterprise networks are complex environments, with numerous components often under the control of teams outside the Security Team. During an incident, it is critical that responders understand the network topology and have the most current information policy and device information available to them.

Network documentation is incomplete and out-of-date; security teams need a way to quickly and efficiently gather actionable network intelligence.

The DFLabs and Tufin Solution.

Harness the vast amount of network intelligence available from Tufin, along with the automation, orchestration and measurement power of DFLabs IncMan.

Tufin Orchestration Suite together with DFLabs IncMan provides joint customers with an automated means to gather actionable network intelligence, a task which would otherwise need to be performed manually, taking up valuable analyst time when every minute counts. This results in an overall decrease in the mean time to respond (MTTR) to a computer security incident, saving the organization both time and potential financial and reputational loss.

DFLabs IncMan SOAR and Tufin Orchestration Suite solve these specific challenges:

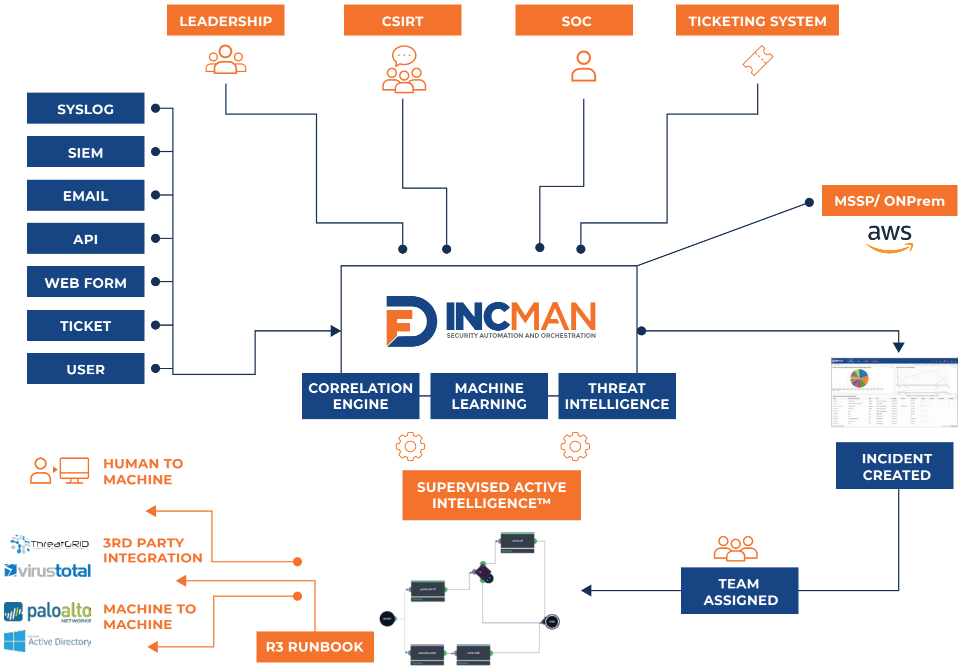
- How can I get a current list of network devices?
- How can I get a current list of rules and polices?
- How can I determine the network path from source to destination?

Combining IncMan SOAR, Tufin Orchestration Suite and other security products enables Enterprises to:

- Reduce incident resolution time by 90%
- Maximize security analyst efficiency by 80%
- Increase the number of handled incidents by 300%

Automate.
Orchestrate.
Measure.

DFLabs IncMan SOAR Overview.



About Tufin.

Tufin Orchestration Suite takes a policy-centric approach to security to provide visibility across heterogeneous and hybrid IT environments, enable end-to-end change automation for network and application connectivity and orchestrate a unified policy baseline across the next generation network.

The result is that organizations can make changes in minutes, reduce the attack surface and provide continuous compliance with internal and external/ industry regulations.

The ultimate effect is greater business continuity, improved agility and reduced exposure to cybersecurity risk and non-compliance.

About DFLabs IncMan SOAR.

DFLabs IncMan Security Orchestration, Automation and Response (SOAR) platform automates, orchestrates and measures security operations and incident response tasks, including threat validation, triage and escalation, context enrichment and threat containment.

IncMan SOAR uses machine learning and Rapid Response Runbooks (R^3 Runbooks) as a force multiplier that has enabled security teams to reduce average incident resolution times by 90% and increase incident handling by 300%.

Automate.
Orchestrate.
Measure.

CHALLENGES

- How can I get a current list of network devices?
- How can I get a current list of rules and polices?
- How can I determine the network path from source to destination?

DFLABS AND TUFIN SOLUTION

- List current network devices based on any number of criteria.
- List current rules and policies for any available device.
- Simulate network traffic from source to destination, including path and associated rules.

RESULTS

- Reduce Incident resolution time by 90%
- Maximize security analyst efficiency by 80%
- Increase the number of resolved incidents by 300%

Use Case.

Network traffic between a workstation and a domain controller has been identified as potentially malicious by the organization's UBA platform. The UBA platform generated an alert which was forwarded to IncMan SOAR, causing an incident to be automatically generated.

Based on the IncMan SOAR Incident Template, the following R3 Runbook was automatically assigned and executed to gather additional network intelligence.

The information gathering begins by simulating the network path between the source address and destination address of the potentially malicious network traffic. This information is gathered by two separate Enrichment actions, one which will display this information in a table format, and another which will display the same information in a graphic network path which can be exported and shared or added to reports.

As with information from any other IncMan Enrichment action, each network device on the path between the source address and the destination address is stored within an array which can be used by subsequent actions.

After the path information has been retrieved, an additional Enrichment action is used to retrieve information about each device along the path. This includes information such as device vendor, model, name and IP addresses.

Following the acquisition of the device information, two additional Enrichment actions are utilized to gather additional network intelligence. The first action will retrieve all rules for each network device along the path. Detailed information on each matching rule will be displayed for the analyst, allowing the analyst to assess why the traffic was permitted or denied, what additional traffic may be permitted from the source to the destination, and what rule changes may be appropriate. The second action will retrieve all policies for each network device along the path. Similar to the previous rule information, this information will allow the analyst to assess the configured network policies and determine what, if any, policy changes should be made to contain the potential threat.

Harnessing the power of Tufin Orchestration Suite, along with the additional Orchestration, Automation and Response features of DFLab's IncMan SOAR, organizations can elevate their incident response process, leading to faster and more effective response and reduced risk across the entire organization.

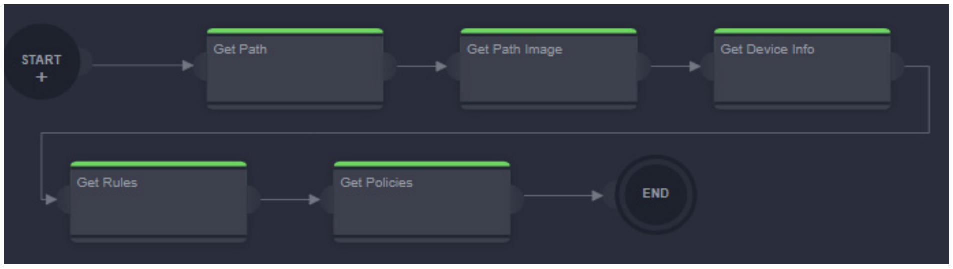
TUFIN ACTIONS

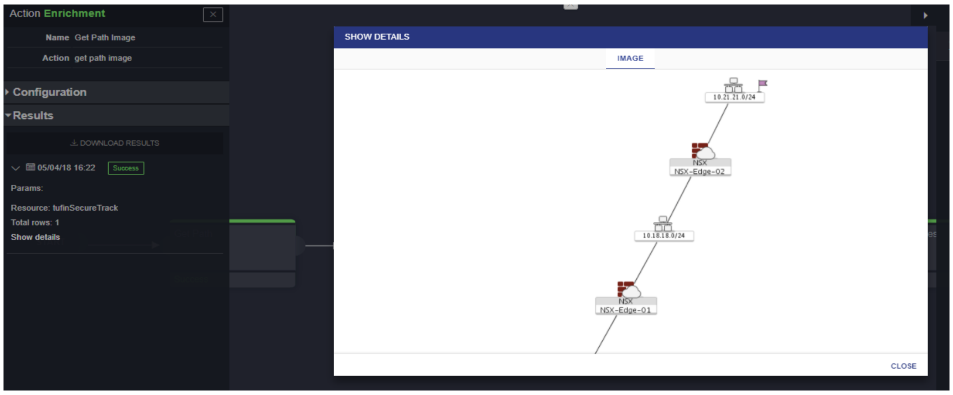
Enrichment

- ✓ Get Devices
- ✓ Get Path
- ✓ Get Path Image
- ✓ Get Policies by Device
- ✓ Get Rule Count

LEARN MORE

For more information on how to take your incident response to the next level with DFLabs IncMan SOAR, contact your DFLabs representative or visit www.dflabs.com.





Name Get Path Image

Action get path image

05/04/18 16:22

Params:

Resource: tufinSecureTrack

Total rows: 1

Show details

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	–	+39 037 832 416
E	–	sales@dflabs.com

About Tufin.

Tufin® is the leader in Network Security Policy Orchestration for enterprise cybersecurity. More than half of the top 50 companies in the Forbes Global 2000 turn to Tufin to simplify management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures.

Enterprises select the company's award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2,000 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries.

Find out more at www.tufin.com.
Follow Tufin on Twitter @TufinTech.

a

Automate.
Orchestrate.
Measure.

tufin | DFLABS
CYBER INCIDENTS UNDER CONTROL