INTEGRATION BRIEF

DFLabs and Javelin AD Protect:

Allow attackers to contain themselves.

Allow attackers to contain themselves with Javelin AD Protect and IncMan SOAR.

DFLABS.COM

Automate.
Orchestrate.
Measure.

JAVELIN

DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Microsoft Active Directory is a pervasive and complex service which is relied upon by both organizations and attackers on a daily basis. Attacks on Active Directory are notoriously difficult to detect with traditional detection technologies. However, once successful they can provide attackers with access to all the organizations most critical assets.

The integration between DFLabs IncMan SOAR and Javelin AD Protect combines advanced Active Directory detection and response technology with cutting-edge orchestration and automation to enable organizations to respond almost instantaneously to Active Directory attacks. AD Protect's advanced protection and IncMan SOAR's R3 Runbooks combine to allow attackers to contain themselves before the security team would even have time to acknowledge the alert.

Enable organizations to respond almost instantaneously to Active Directory attacks.

The Problem.

Organizations of all sizes rely on Microsoft Active Directory as the backbone of their identity and access management. As much as organizations rely on Active Directory, many do not fully understand its complexities or the best practices for hardening its configurations. Attackers too have come to rely on Active Directory as a potential gold mine of information. From reconnaissance and information gathering to authentication attacks, Active Directory can provide attackers with the keys to an organization's most critical resources.

Because Active Directory is an open service by design, attacks on Active Directory are especially difficult to detect. Most often, attacks involving Active Directory are detected based on other actions taken by the attacker, and long after the damage is done.

DFLABS.COM

The DFLabs and Javelin AD Solution.

The integration between DFLabs IncMan SOAR and Javelin AD Protect combines advanced Active Directory detection and response technology with cutting-edge orchestration and automation to allow organizations to respond almost instantaneously to Active Directory attacks. AD Protect's advanced protection and IncMan SOAR's R3 Runbooks combine to allow attackers to contain themselves before the security team would even have time to acknowledge the alert.

IncMan SOAR's powerful automation and orchestration capabilities allow joint customers to automatically begin enriching the wealth of information gathered by AD Protect, separating benign artifacts from potential indicators of compromise which can be used to identify the attacker and search for additional compromise across the environment.

DFLabs IncMan SOAR and Javelin solve these specific challenges:

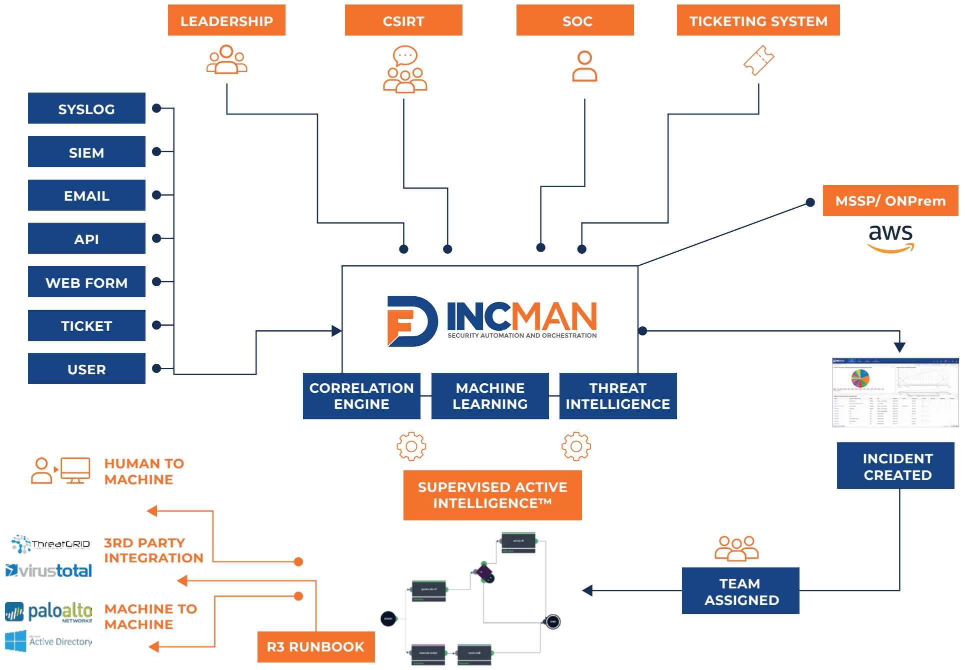
- Active Directory forms the backbone of many organizations IAM
- Configuring and hardening Active Directory is complex and often misunderstood
- Attacks on Active Directory are very difficult to detect

Combining IncMan SOAR, Javelin AD Protect 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 Javelin AD Protect.

Javelin AD Protect controls the attacker's perception autonomously at the endpoint with no agent, and identify the Dark Corners the attacker favors. AD Protect achieves definitive alerts on post-exploitation activity—the most important part of the breach—to stop reconnaissance, credential theft, and lateral movement. Once a threat is detected, AD Protect gathers relevant artifacts automatically before an attacker can erase them, reducing time and effort to investigate the breach.

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

- Active Directory forms the backbone of many organizations IAM
- Configuring and hardening Active Directory is complex and often misunderstood
- Attacks on Active Directory are very difficult to detect

DFLABS AND JAVELIN AD PROTECT SOLUTION

- Detect Active Directory reconnaissance and attacks
- Immediately contain attackers to mitigate the threat
- Enrich attack indicators automatically

RESULTS

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

Use Case.

An attack is detected by Javelin AD Protect, causing an incident to be generated within IncMan SOAR. The Runbook begins by retrieving the report generated by AD Protect when the attack was detected. This report contains a wide variety of information which can be enriched by IncMan SOAR or used by an analyst to perform further investigation. After retrieving the report generated by AD Protect, the Runbook checks to see if any hash values or network connection information is present in the report. If either hash values or network connection information is present in the report, the Runbook will query the organization's threat intelligence provider of choice to determine if the hash values or IP addresses are malicious. If any hash values or IP addresses have associated intelligence above a certain threshold, the runbook will automatically block the given IP addresses or hash values. Finally, the runbook will query the organization's EDR solution for any of the hash values or IP addresses which have been determined to be malicious to determine if any other endpoints on the network have these artifacts associated with them.

Simultaneously, the Runbook will gather any user accounts from the report generated by AD Protect and extract any domain accounts. The Runbook will then query Active Directory for the attributes of any domain user account found on the potentially compromised host. For each domain account found, the analyst will be prompted with a User Choice decision asking if they would like to reset the user's password. If the analyst chooses to reset the user's password, a separate Runbook will be executed on the specified user account to reset the password to a random string and email the user with the new temporary password.

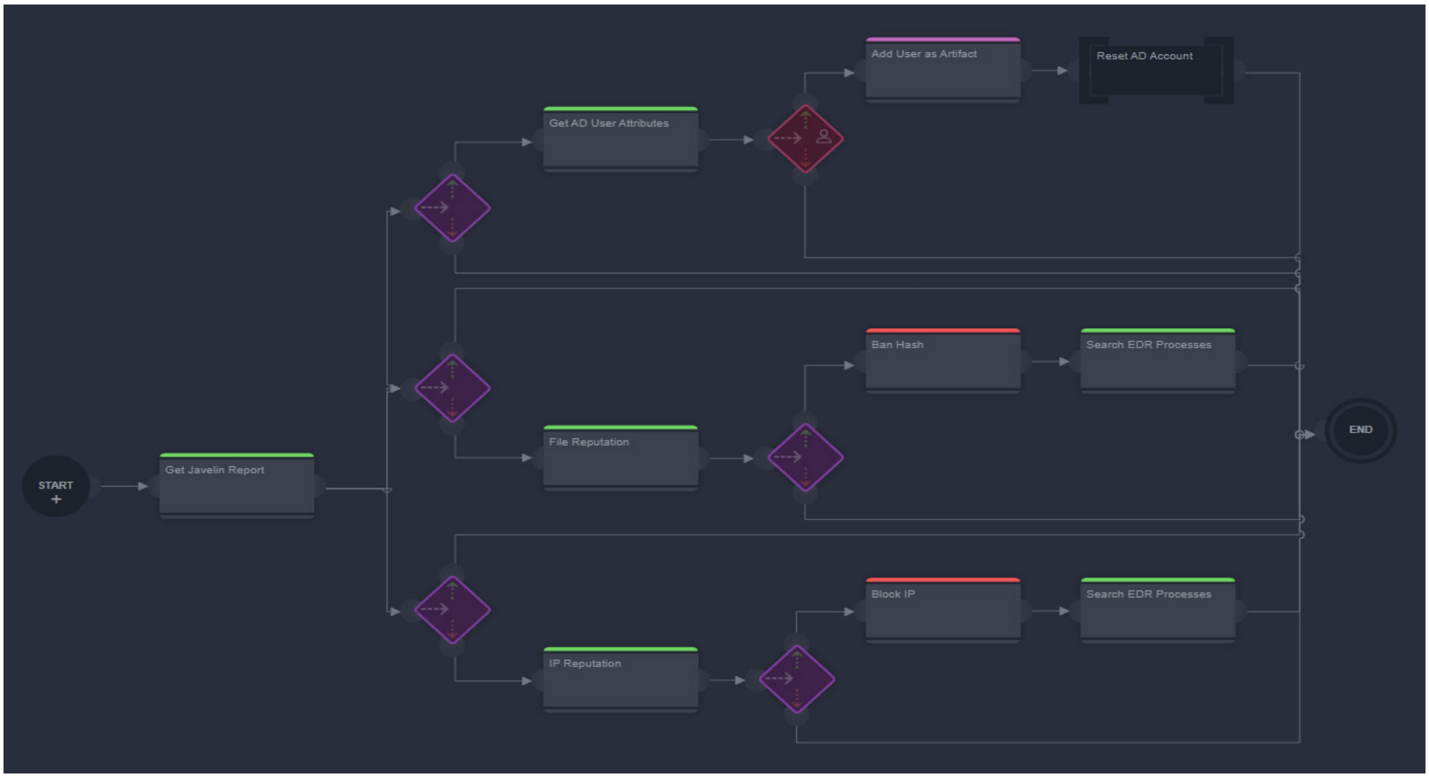
JAVELIN AD PROTECT ACTIONS

Enrichment

✓ Get Report

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.



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 Javelin Networks.

Javelin Networks is now a Symantec company.

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives.

Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and familiesrely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices.

Symantec operates one ofthe world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

For additional information, please visit www.symantec.com or formally www.javelin-networks.com/ad-protect.

Automate.
Orchestrate.
Measure.

JAVELIN

DFLABS
CYBER INCIDENTS UNDER CONTROL