INTEGRATION BRIEF

DFLabs & Micro Focus ArcSight:

Add Context and Enrich Alert Information for a More Effective Response.

Increase the efficiency and effectiveness of your response by adding context and enrichment from ArcSight data.

DFLABS.COM

Automate.
Orchestrate.
Measure.

MICRO FOCUS® | DFLABS CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Organizations are increasingly turning to SIEM technologies to help manage, correlate and alert on potential events from the large quantity of data generated by the many log sources in today's security ecosystem. Once data is correlated and an alert is generated, enriching the alert data is often a manual task which consumes a significant amount of analysts' time.

DFLabs IncMan SOAR and Micro Focus ArcSight bring SOAR and SIEM together to allow rapid, informed responses to security incidents based on enriched, actionable information. IncMan SOAR allows users to automatically pivot from the initial alert to gather increase insight in to the activity within the organization.

DFLabs IncMan SOAR and Micro Focus ArcSight bring SOAR and SIEM together to allow rapid, informed responses to security incidents based on enriched, actionable information.

The Problem.

Organizations are generating more log data than ever before. Organizations are increasingly turning to SIEM technologies to help manage, correlate and alert on potential events from this large quantity of data. Once data is correlated and an alert is generated, enriching the alert data is often a manual task which consumes a significant amount of analysts' time. Pivoting from a single alert, or from enriched information, is often also a manual process, requiring many more custom written queries within the SIEM. Enriched and additional data must then be correlated manually by the analyst before it becomes actionable.

The DFLabs and ArcSight Solution.

DFLabs IncMan SOAR and Micro Focus ArcSight bring SOAR and SIEM together to allow rapid, informed responses to security incidents based on enriched, actionable information. IncMan SOAR allows users to automatically query ArcSight to pivot from an initial alert to gather increase insight in to the activity within the organization. IncMan SOAR also allows users to enrich information retrieved from ArcSight, such as IP addresses, hostnames and domains, using any number of IncMan's other integrations.

DFLabs IncMan SOAR and ArcSight solve these specific challenges:

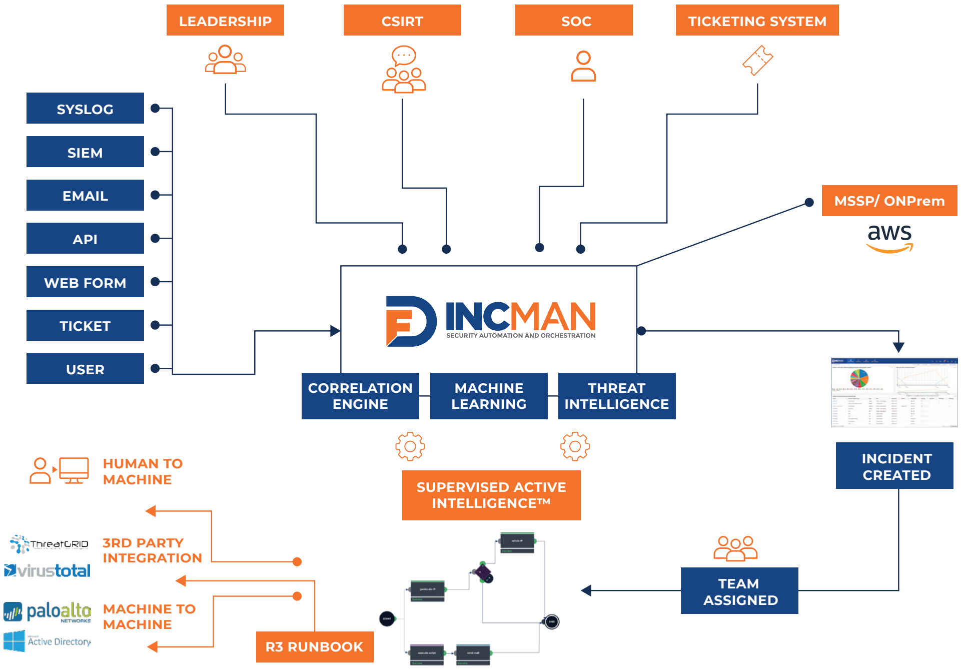
- How can I use my SIEM logs to add context to a security event?
- How can I enrich information from the initial security alert?
- How can I pivot from the intitial security alert to further my investigation?

Combining IncMan SOAR, ArcSight 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 ArcSight.

ArcSight is an industry-leading Security Information and Event Management (SIEM) solution from Micro Focus. ArcSight collects and analyzes events from across systems and security tools. It detects security threats in real time so that analysts respond quickly, and it scales to meet demanding security requirements. ArcSight's advanced distributed correlation engine, helps security teams detect and respond to internal and external threats, reduces response time from hours or days to minutes.

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%.

CHALLENGES

- How can I use my SIEM logs to add context to a security event?
- How can I enrich information from the initial security alert?
- How can I pivot from the initial security alert to further my investigation?

DFLABS AND ARCSIGHT SOLUTION

- Automatically query data from multiple log sources
- Enrich event information using third-party solutions
- Pivot from the initial event to find additional indicators

RESULTS

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

Automate.
Orchestrate.
Measure.

Use Case.

A Web Application Firewall (WAF) has observed a potential attack against an application server in the organization's DMZ. The runbook begins by performing basic enrichment on the source IP address of the malicious traffic. This basic enrichment is followed by a query for IP reputation information on the source IP address from the organization's threat reputation service of choice.

Following the threat reputation search, ArcSight is queried for any other events which have been recently generated by the source IP address. If ArcSight returns any other recent events generated by the source IP address, or the source IP address has a negative threat reputation, the severity of the incident is automatically upgraded to High. The analyst is then presented with a user choice decision to determine if the source IP address should be blocked at the perimeter firewall. If the analyst chooses to automatically block the source IP address, a ticket will be created in ArcSight ESM to notify the appropriate teams to follow up on the emergency change according to the organization's policies.

These actions are followed by a second query to ArcSight, this time for any other recent events involving the web application server. If ArcSight returns any other recent events generated from the web application server, the severity of the incident is automatically upgraded to High (unless it has already previously been upgraded). The runbook concludes by performing a query of the organization's endpoint detection solution for all recent events from the web application server. This information will be retained for review by the analyst during the investigative process.

ARCSIGHT ACTIONS

Enrichment

- ✓ Get Active List Entries
- ✓ Search Into Events

Containment

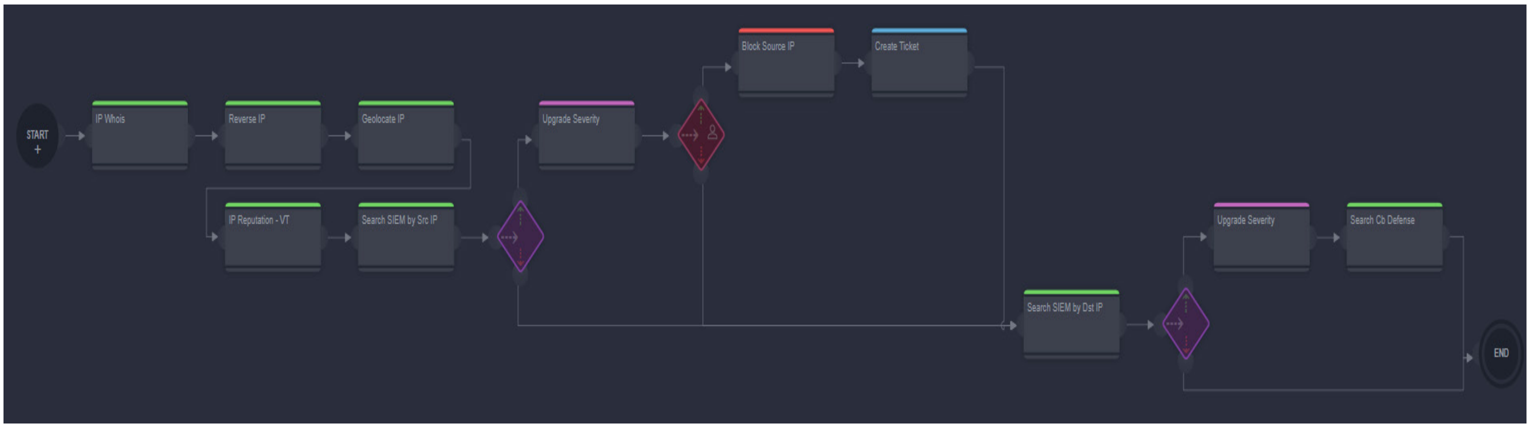
- ✓ Add Active List Entries
- ✓ Clean Active List Entries

Notification

- ✓ Create Ticket
- ✓ Get Ticket
- ✓ Update Ticket

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 Micro Focus.

Micro Focus is a leading global enterprise software company uniquely positioned to help customers extend existing investments while embracing new technologies in a world of Hybrid IT. Providing customers with a world-class portfolio of enterprise-grade scalable solutions with analytics built-in, Micro Focus delivers customer-centered innovation across Hybrid IT Management, Enterprise DevOps, Security & Data Management, and Predictive Analytics.

For more information visit www.microfocus.com and follow us on Twitter at @MicroFocusSW.

Automate.
Orchestrate.
Measure.

MICRO FOCUS® | DFLABS CYBER INCIDENTS UNDER CONTROL