INTEGRATION BRIEF

DFLabs and Check Point: Bringing Next-Generation Protection to Next-Generation Threats.

Provide users with the capability to integrate Next-Generation firewalls and other disperse technologies with IncMan SOAR to protect against Next-Generation threats.

DFLABS.COM

Automate.
Orchestrate.
Measure.

Check Point® SOFTWARE TECHNOLOGIES LTD.

DFLABS CYBER INCIDENTS UNDER CONTROL

Solution Overview.

DFLabs together with Check Point Software Technologies provides users with the capability to integrate their Next-Generation firewalls with other disperse technologies within their security stack. Checkpoint's unified security management system enables organizations to gain greater visibility across their entire environment and allows for full control over environmental attributes such as users, applications, and connection types.

Equipped with their advanced network threat protection solution, Sandblast, organizations are provided with evasion-resistant malware detection by utilizing threat emulation and CPU-level inspection to deliver complete protection against next generation advanced cyber-attacks.

Today's networks are under attack by more sophisticated actors and their tactics are becoming harder to detect and protect against.

The Problem.

Today's networks are under attack by more sophisticated actors and their tactics are becoming harder to detect and protect against. Whether the risks come from external sources or are internal to an organization, the need for greater security capabilities is at an all-time high.

Almost every user in an organization must connect to the Internet to access business resources. As more organizations move their operations to the cloud, the ability to have full visibility of its users and their resources have added a new level of difficulty for security teams.

Between access management, application control, and the advanced sophistication of attack methods there seem to be risks around every corner.

Unfortunately, most IT organizations are operating with inadequate tools for the job. Security professionals must focus on closing this gap to prevent any opportunity for a breach to occur. By creating innovation and implementing the most recent threat prevention strategies security teams can stay one step ahead of their adversaries.

The DFLabs and Check Point Solution.

The integration between DFLabs and Checkpoint brings next-generation response efforts to a potential incident. By querying Checkpoint for IP and Domain information, IncMan has a solid foundation to begin automating containment actions where necessary.

This vital information early on in an investigation can help organizations contain an incident before it becomes a breach. Incorporating Checkpoint's security capabilities into the additional technologies in an organization's security stack, allows for containment efforts to stretch far beyond an organization's perimeter.

DFLabs IncMan SOAR and Check Point solve these specific challenges:

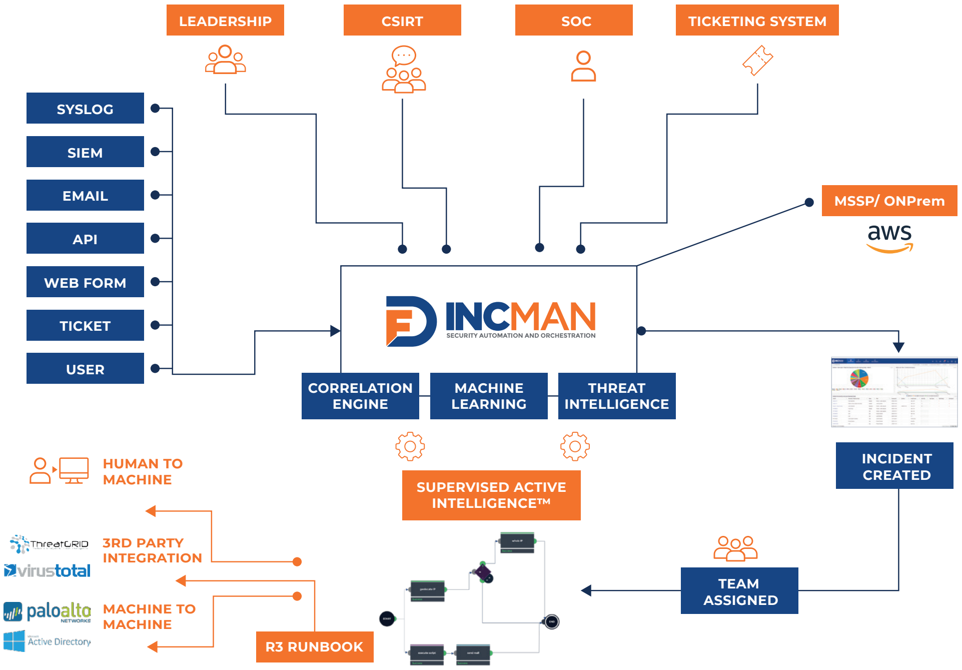
- Network complexity makes it difficult to track access to sensitive data and resources
- More sophisticated threats require multiple toolsets to provide complete protection
- Most organizations have not adopted the latest in threat detection and remediation tactics

Combining IncMan SOAR, Check Point 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 Check Point.

Check Point Software Technologies Ltd. is a multinational provider of software and combined hardware and software products for IT security, including network security, endpoint security, mobile security, data security and security management.

Their product line continues to evolve with their latest focus on large-scale and fast-moving attacks across mobile, cloud and on-premise networks which easily bypass the conventional, static detection-based defenses being used by most organizations today.

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 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

- Network complexity makes it difficult to track access to sensitive data and resources
- More sophisticated threats require multiple toolsets to provide complete protection
- Most organizations have not adopted the latest in threat detection and remediation tactics

DFLABS AND CHECK POINT SOLUTION

- Track access to sensitive data and resources
- Next-Generation protection technologies for Next-Generation threats
- Native Active Directory integration for identity awareness

RESULTS

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

Use Case.

An alert is received from Check Point which indicates a host has been in communication with a potentially malicious domain. IncMan SOAR automatically begins to gather information regarding the domain and IP address. Once the reputation of both the domain and IP address is checked, IncMan will comes to its first set of conditional actions.

If either the domain or IP address produces a risk score of 50 or above, IncMan will automatically block the domain and IP address at the Check Point devices. Once the IP and or domain is blocked, IncMan will query the EDR solution to see if there had been any other communication with the IP or domain in their environment in the last week.

If this query returns any additional observations, the incident will be upgraded to a Priority 1 incident and the additional hosts observed will be added as incident artifacts. IncMan will engage the EDR solution to quarantine the affected host and the user's account will have its password reset by a randomly generated password. An email notification will be sent out to the responsible teams for further follow up and remediation tasks if necessary

CHECK POINT ACTIONS

Enrichment

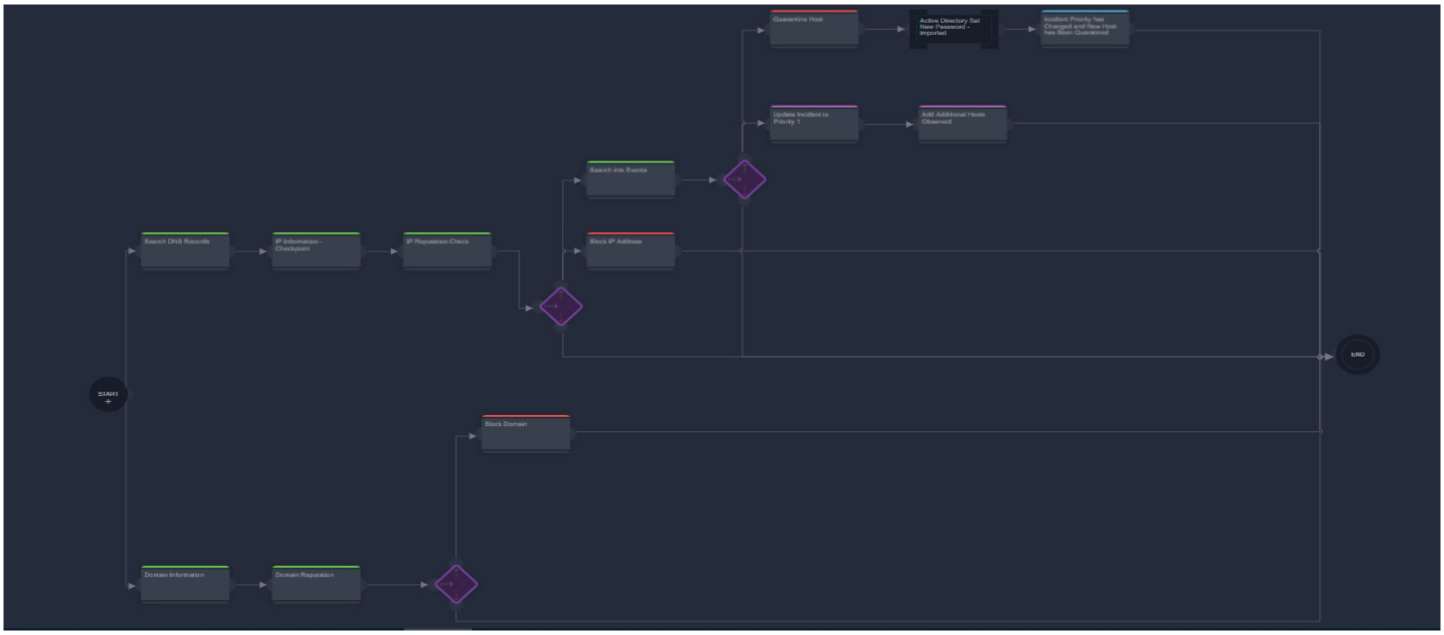
- ✓ User Attributes
- ✓ IP Information
- ✓ Domain Information

Containment

- ✓ Block IP
- ✓ Unblock IP
- ✓ Block Domain
- ✓ Unblock Domain
- ✓ Lock User
- ✓ Unlock User

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.


START
Search DNS Records
IP Information - Checkpoint
IP Reputation Check
Search into Events
Block IP Address
Quarantine Host
Active Directory Set New Password - imported
Incident Priority has Changed and New Host has Been Quarantined
Update Incident to Priority 1
Add Additional Hosts Observed
Block Domain
Domain Information
Domain Reputation
END

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 Check Point.

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally.

Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks.

Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system.

Check Point protects over 100,000 organizations of all sizes

For more information visit www.checkpoint.com or connect with us on Twitter @CheckPointSW.

Automate.
Orchestrate.
Measure.

Check Point®
SOFTWARE TECHNOLOGIES LTD.

DFLABS
CYBER INCIDENTS UNDER CONTROL