.

DFLabs + Cisco ISE

Enhance Your SecOps With Security Automation

Keep Your Cyber Incidents Under Control.

Benefits

- All-in-one platform to improve your own processes (SOPs)
- Easily orchestrate your tools leveraging Open Integration Framework
- Save time and focus on real Threats
- Automate mundane tasks
- Reduce false positives
- Respond to attacks in less time
- Centralize threat intelligence

Features

- Playbooks to efficiently improve SecOps processes
- Accurate & automated enrichment of alarms
- Progressive automation of time-consuming activities and mundane tasks
- Immediate detailed Incident reports with related IOC's, timeline, and corrective actions executed
- KPIs dashboards for analysts, SOC manager, CISO, audit managers, etc.
- Native Multi-Tenancy platform

The Challenge.

Organization's users are becoming more mobile as the world becomes more digitally interconnected. This shift from purely on-prem defense strategies to a complicated mix between traditional defenses and the need to extend beyond our common boundaries has created a difficult dilemma for network defenders. As more users and infrastructures are migrating to the cloud and Internet threats become more sophisticated, the need for greater visibility, intelligence, protection, and rapid response has left the industry scrambling to keep up.

SOAR Starts Where Detection Stops.

DFLabs' IncMan SOAR platform helps Enterprises and MSSPs improve their security operations processes. IncMan's unique triage capability reduces the number of false positives and handles suspicious events that require deeper analysis.

Joint Solution.

A new approach is needed to stay ahead of the curve and that is the reason why Cisco and DFLabs have combined their industry-leading solutions to utilize IncMan SOAR with Cisco ISE Session, Policy, and Security Group information during security investigations.

Enrichment, Containment leveraging Cisco ISE actions:

- **Get Sessions (Enrichment) - Gather session information from Cisco ISE**
- **List Policies (Enrichment) - List all available ISE policies**
- **List Security Groups (Enrichment) - List all available security groups**
- **Get Policies Endpoints (Enrichment) - List endpoints associated with policies**
- **Apply Policy (Containment) - Create a new policy**
- **Clear Policy (Containment) - Remove an existing policy**
- **Get Endpoints (Enrichment) - List all available endpoints**
- **Get Endpoint Identity Groups (Enrichment) - List all available endpoint identity groups**
- **Get Internal Users (Enrichment) - List all available internal user**

About Cisco ISE.

A critical component of any zero-trust strategy is securing the workplace that everyone and everything connects to. Cisco Identity Services Engine (ISE) enables an automated and dynamic approach to policy enforcement by simplifying the delivery of highly secure network access control. ISE empowers software-defined access and automates network segmentation within IT and OT environments. Cisco ISE allows you to provide highly secure network access to devices and users. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as threats, vulnerabilities and user and device identities with integrated solutions from Cisco technology partners, so you can identify, contain, and remediate threats faster.

How Cisco ISE and IncMan SOAR Work Together.

IncMan facilitates visibility and management across the entire incident response workflow with the concept of Rapid Response Playbooks. Playbooks are a collection of actions that can be executed by the user in a linear or conditional fashion. Actions can be converted to tasks and assigned to specific analysts or investigators. Each Action can be flagged for supervisory approval as part of the response protocol if desired. Automatic Actions are able to execute Human to Machine instructions to external systems and applications. Automatic Action can take the form of:

- Interaction with Firewall software to automate the blocking/unblocking of TCP services, URLs, IP addresses, and applications;
- Interact with user authentication system (e.g., LDAP or Active Directory) to block or unblock users, limit user/group privileges, reset/change user passwords, etc;
- Interact with SIEM products executing search during a specific time frame;
- Interact with GEOIP or Threat Feed services;
- Generate specific reports or notifications;
- All Automatic Actions results are saved inside the Playbook for each incident.
- Automatic Actions can be executed in Machine to Machine mode for example specific details can be extracted from an alert sent to IncMan and used to pre-populate appropriate Automatic actions. In this scenario, when an alert is triggered for example by a SIEM, IncMan creates an incident and executes appropriate enrichment and containment actions.

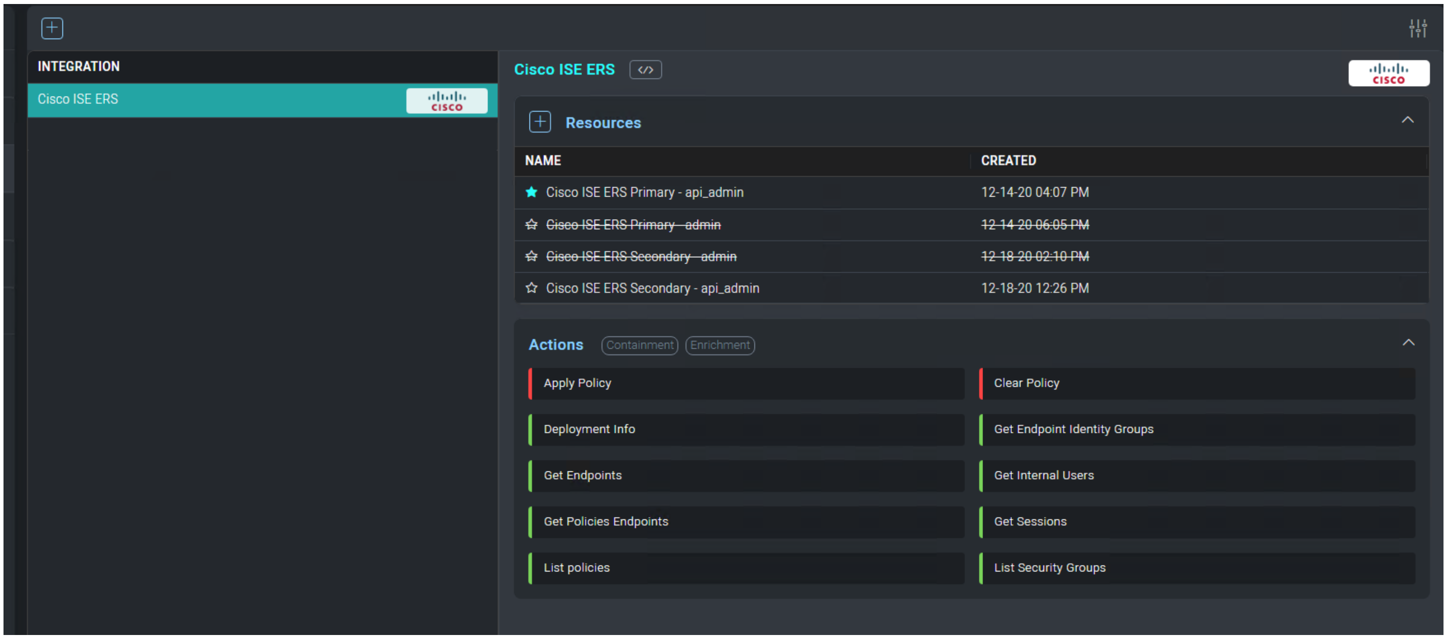
The status of each Playbook can be monitored by the incident handlers of each incident if they have sufficient permission (IncMan's RBAC is very granular). Every task status and its progress can be monitored from a single point via the Playbook management interface.

Additionally, the solution offers workflow automation in order to streamline processes with additional systems that integrate with IncMan SOAR. There is a possibility to define different categories and subcategories as well as actions. For each action, the user has the ability to define and execute the action manually or automatically as well as designate an approving authority before the action is permitted. When defining the automatic action, there is a possibility to choose if the action will be set in order to enrich or contain the incident or even the ability to create a custom script action. Additionally, IncMan is capable of granular reporting of incident KPIs as well as a host of user-configurable reports that are entirely customizable.

How Automation Works?

Playbooks improve SecOps processes and allow analysts to follow Standard Operating Procedures (SOP).

A playbook is a graphical definition of a workflow to resolve an incident or complete an investigation. Within these processes, Cisco ISE actions can be easily called up via API connectors. The role of automation in SOAR is to ease the burden of cybersecurity organizations by automating repetitive behavior and recurring tasks. The degree of automation can be adjusted, and security teams can determine whether they want some tasks to include human interaction (extremely fundamental in some processes) or if they want all of their tasks to be fully automated. With the help of automation, security teams can deal with potential alerts in a much faster, more effective manner, and also have total control of the tasks where it’s required to include human interaction. The degree of automation is completely adjustable, and security teams can choose to fully automate time-consuming and repetitive tasks and also include human interaction in tasks that require expert attention.



INTEGRATION

Cisco ISE ERS

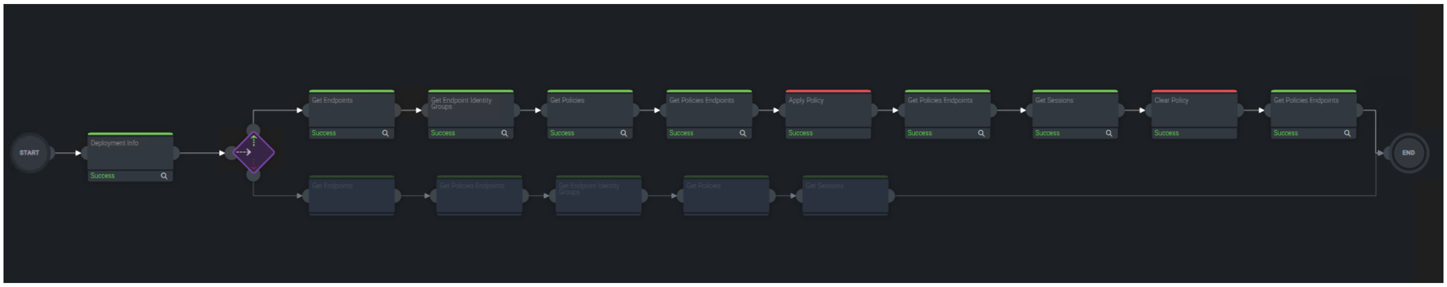
Cisco ISE ERS </>

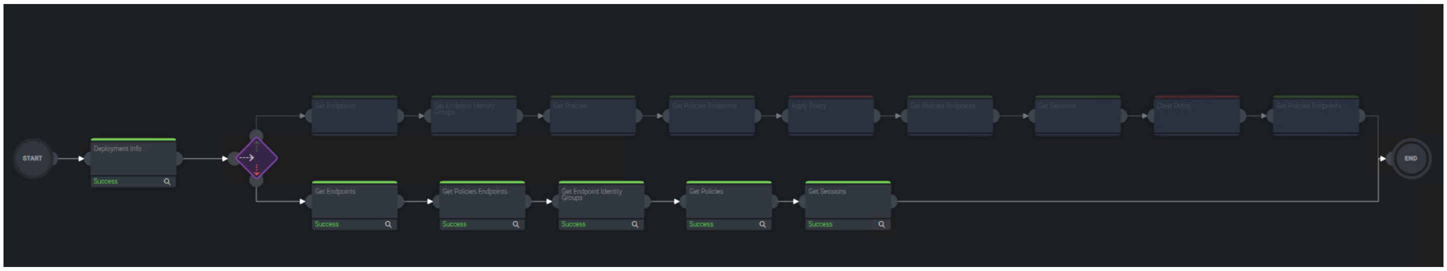
Resources

NAME	CREATED
★ Cisco ISE ERS Primary - api_admin	12-14-20 04:07 PM
☆ ~~Cisco ISE ERS Primary - admin~~	~~12-14-20 06:05 PM~~
☆ ~~Cisco ISE ERS Secondary - admin~~	~~12-18-20 02:10 PM~~
☆ Cisco ISE ERS Secondary - api_admin	12-18-20 12:26 PM

Actions (Containment) (Enrichment)

Apply Policy	Clear Policy
Deployment Info	Get Endpoint Identity Groups
Get Endpoints	Get Internal Users
Get Policies Endpoints	Get Sessions
List policies	List Security Groups





Ease of Integration.

IncMan SOAR allows clients and partners to create an integration with various tools in 3 days average time, with no advanced coding experience required beforehand. Thanks to Orchestration, you can connect all the technologies SecOps need through API connectors. This enables replication and improvement of SOC processes, and security analysts have all the information they need on a unique SOAR platform. This way you can benefit from the full power of Cisco ISE by calling up their actions within playbooks to respond quickly to threats.

Connectors are written with python, and customers can easily add actions to existing integrations without the need to modify existing code. Open Integration Framework defines all integrations at the action level, not as one monolithic file. The execution of each integration is performed in a unique Docker container and easily configured from within the integration file, providing additional security and eliminating the risk of conflicting libraries. There are no limits to the integrations you can create including your own script - Cyber - Anti-fraud - Industrial - IoT - Daemons and beyond. The field of application of daemons is almost unlimited. They are not just security activities, but they can also be applied to IT incidents or simple daily monitoring processes.

Summary.

With Cisco ISE and DFLabs, security teams have a solution to improve Standard Operating Procedures that can keep up with the scale of your infrastructure. This combined approach offers a number of benefits, including:

Improve SecOps process

With DFLabs and Cisco, users have a single, consistent method to add observables to configured blocklists, distribute to the Cisco ISE solution and create standardized workflows based on these insights.

Optimizing security response

SOAR allows security teams to automate repetitive, mundane, and time-consuming tasks by effectively tackling alerts from detection to resolution in a fast and concise manner. IncMan's TRIAGE Capability allows the reduction of false positives and other red flags raised by an elevated number of suspicious events that have to be inspected and can be achieved with different techniques of pre-processing based on automation, machine learning, correlation, and aggregation of events.

Faster and more efficient incident reporting

IncMan SOAR allows analysts to be more effective as it creates extremely fast incident reports that only take a couple of minutes. SOAR provides an immediate and detailed incident report with corrective actions executed.

Probatory role and Chain of custody

DFLabs case management also handles forensics, the evidentiary chain of custody of the incident response processes, including but not limited to, reports, evidence preservation, integration with forensic technology, Incident Artifact, IOCs, etc. DFLabs' evidentiary and probationary role provides in-depth information in over a hundred customizable Case Management fields.

Multi-Tenancy and clustering

IncMan SOAR applies a sophisticated multi-tenant engine, which is specifically designed to support both MSSPs and also adjust to complex corporate environments.

About Cisco.

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more on The Network and follow us on Twitter.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

About DFLabs.

DFLabs is an award-winning and recognized global leader in security orchestration, automation, and response (SOAR) technology. The company's management team has helped shape the cybersecurity industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121. Its flagship product, IncMan SOAR, is multi-patented, and it has been adopted by Fortune 500 and Global 2000 organizations worldwide. DFLabs has operations in EMEA Americas and APAC. For more information, visit **www.dflabs.com**.

CONTACT US

E – sales@dflabs.com