DFLabs + Qualys

Seamlessly Orchestrate All Your Tools and Empower SecOps

Keep Your Cyber Incidents Under Control.

Benefits

- All-in-one platform to improve your own process (SOP)
- 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

- Runbooks to efficiently improve SecOps processes
- Accurate & automated enrichment of alarms
- Progressive automation of time-consuming activities and mundane tasks
- Alarm Triage Management to empower reduction of false positives
- Immediate detailed Incident reports with related IOC's, timeline and corrective actions executed
- KPIs dashboards for analyst, SOC manager, CISO, audit manager. ecc
- Native Multi-Tenancy platform

The Challenge.

Nowadays, cyber threats are becoming more and more difficult to trace, which leaves analysts with the difficult task of investigating and containing each threat as it arrives in real-time. Security operations require the merging of intelligence, both from in-house staff and technological solutions. Cyber attacks are becoming more unpredictable than ever, and that exact unpredictability led to the formation of the following challenges that prompted the birth of a whole new cybersecurity technology:

- **An increasing number of alerts**
- **False positives and false negatives**
- **Overwhelming workload for SecOps and SOCs**
- **Sophisticated attacks with no recognizable patterns**

SOAR Starts Where Detection Stops.

DFLabs' IncMan SOAR (Security Orchestration, Automation and Response) 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.

With DFLabs' IncMan SOAR and Qualys solutions, analysts can orchestrate and efficiently implement a more effective security solution that can keep up with the pace of emerging threats. Thanks to the API, you can easily manage Qualys solutions in your processes to enrich and validate alarms.
Here are some actions that can be orchestrated and progressively automated, thanks to IncMan SOAR.

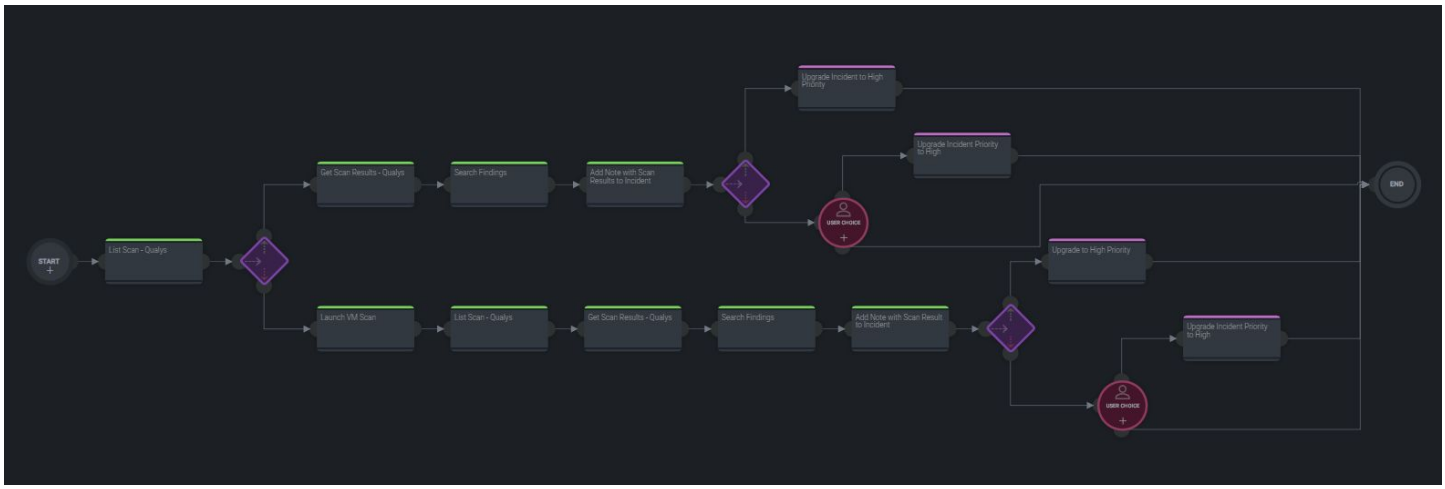
Enrichment leveraging Qualys actions:

List Scan – generates a list of previously executed scas

- **Launch VM Scan – launch a new VM scan**
- **Manage VM scans – Manage existing VM scans**
- **Get Scan results – gather results of an executed scan**
- **Add asset**
- **List Asset Group – generate a list of all asset groups**
- **List asset – generates a list of all available assets**
- **Get scanner details – gather details of a specific scanner**
- **List option profiles – generates a list of all available option profiles**

By leveraging Qualys solutions to derive threat intelligence from tracked security observables in DFLabs' IncMan SOAR, enrich alarms and block threats, analysts can implement a more effective security solution, create detailed reports with related IOC's, timeline, corrective actions and other information.

Example: Enrichment and Prioritization with Qualys.



Starting from a possible suspicion of compromise you could immediately verify the correlation between the vulnerable surface of the machine that you are investigating and the metadata part of the received alert.

When did you scan the machine last time?
If it was over a week ago IncMan automatically updates the results by triggering a new scan.

Then IncMan seeks the findings looking for a vulnerability that matches the potential exploit that you are investigating

Is there a match?
If yes IncMan instantly increases the priority of the incident to a high level.
If not, IncMan interoperates with the security analyst to decide how to treat the incident prioritization

How Automation Works?

Runbooks improve SecOps processes and allow analysts to follow Standard Operating Procedures (SOP).
Runbook is a graphical definition of a workflow to resolve an incident or complete an investigation within these processes QUALYS actions can be easily called up via API connectors.

The role of automation in SOAR (Security Orchestration Automation and Response) is to ease the burden of cyber security 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.

Via automation, security teams can deal with potential alerts in a faster, more effective manner, and also have total control of the tasks where they wish 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.

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 permits 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 QUALYS solutions by calling up their actions within runbooks to respond quickly to threats.

Summary.

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

Improve SecOps process

With DFLabs and Qualys, users have a single, consistent method to add observables to configured block lists, distribute to all qualys solutions 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. Via case management, clients can stay on top of all the relevant information of a cyber incident, including the elements which have been found, the type of attack that was intended, and who made the attack. 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 Qualys.

Qualys, Inc.www.qualys.com is a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions with over 15,700 active customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes, and substantial cost savings.

About DFLabs.

DFLabs www.dflabs.com is a pioneer in security orchestration, automation and response (SOAR) technology. 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. Its flagship product, IncMan SOAR, has been adopted by Fortune 500 and Global 2000 organizations worldwide and awarded three Patents in the USA. DFLabs has operations in EMEA, North America and APAC. IncMan SOAR platform is an award-winning SOAR platform and DFLabs is honored to be acknowledged by a number of leading security award programs.

CONTACT US

IT – +39 0373 82416 UK – +44 203 286 4193 E – sales@dflabs.com