The Complete Guide to

Security Orchestration, Automation and Response(SOCGUARD)

by

Andisheh Pardazan Goya System

(+98)9219427704

Security Operation Center GUARD

(SOCGUARD)

Introduction

Gartner defines SOAR as a technology that enables the organization to take inputs from various source and apply workflow aligned to process and procedure.

These can be orchestrated via integrations with other technologies and automated to achieve the desired outcome and greater visibility. Additional capabilities include case and incident management features, the ability to manage threat intelligence, dashboards, and reporting, analytics that can be applied across various functions. SOCGUARD tools provide machine-powered assistance to human analysts to improve the efficiency and consistency of people and processes by significantly enhancing security operations activities like threat detection and response.

Why SOCGUARD?

Like many new tools for cyber security, it is crucial to know what problems drove for invention of SOCGUARD before deep diving into the definition of SOCGUARD. The five key problems the SOCGUARD market has evolved to address are as follows:

01

Organizations are being forced to achieve workload with less skilled analysts and high expectations.

02

Alerts consume most of the analyst time with similar analysis and false alarms and performing the same tasks to determine the accuracy of the alerts.

03

Security incidents are becoming more expensive, pushing organizations to find new ways to reduce the meantime to detection and the meantime to resolution further.

04

Security operations are naturally difficult to measure and manage effectively.

05

Tribal knowledge is genetically difficult to codify and often leaves the organization with personnel changes.

What SOCGUARD can do?

One of the added advantages of SOCGUARD is its flexibility. SOCGUARD can be used to simplify any number of common tasks, like updating threat databases and responding to alerts.

Key applications:

Manage Vulnerabilities: Correlating log data with threat intelligence to understand what attackers are using and identify vulnerable elements of your infrastructure before they can be compromised.

Coordinate investigations: Unify security data easily and retrieve relevant third-party threat intelligence when you need it. Instant access to external data sources helps analysts in making a precise decision in each investigation.

Respond to incidents: Playbooks, a set of rules enables SOCGUARD platforms to act automatically when an incident occurs. This functionality helps in setting up an automated response for the most common incident types.

Streamline collaboration: Incident investigation and other security processes can grind to a halt when teams aren't able to collaborate easily, such as when teams throughout an organization store data in different formats and use different software. SOCGUARD helps you eliminate these barriers to collaboration.

What SOCGUARD is Not:

A SOCGUARD solution is not a replacement for skilled analysts. Deploying a SOCGUARD solution to replace analysts will inevitably create more risk rather than mitigation. Instead, a SOCGUARD solution should be viewed as an enabler for the security program and security analysts alike.

SOCGUARD solutions are not designed to ingest a large volume of raw events. Instead, SOCGUARD solutions are designed to pick up the incident where SIEM functionality ends, providing anautomated and orchestrated response throughout the Identification Phase, as well as theContainment, Eradication and Recovery Phases.

SOCGUARD is a solution for mitigating security threats through automation which is programmed to collect data about security threats from various sources and respond quickly to the low-level security events without human assistance.

SOCGUARD functions:

Aggregation: The ability to aggregate data across different sources in the form of alerts, or inputs from other technologies such as an alert from a SIEM tool or an email sent to a mailbox.

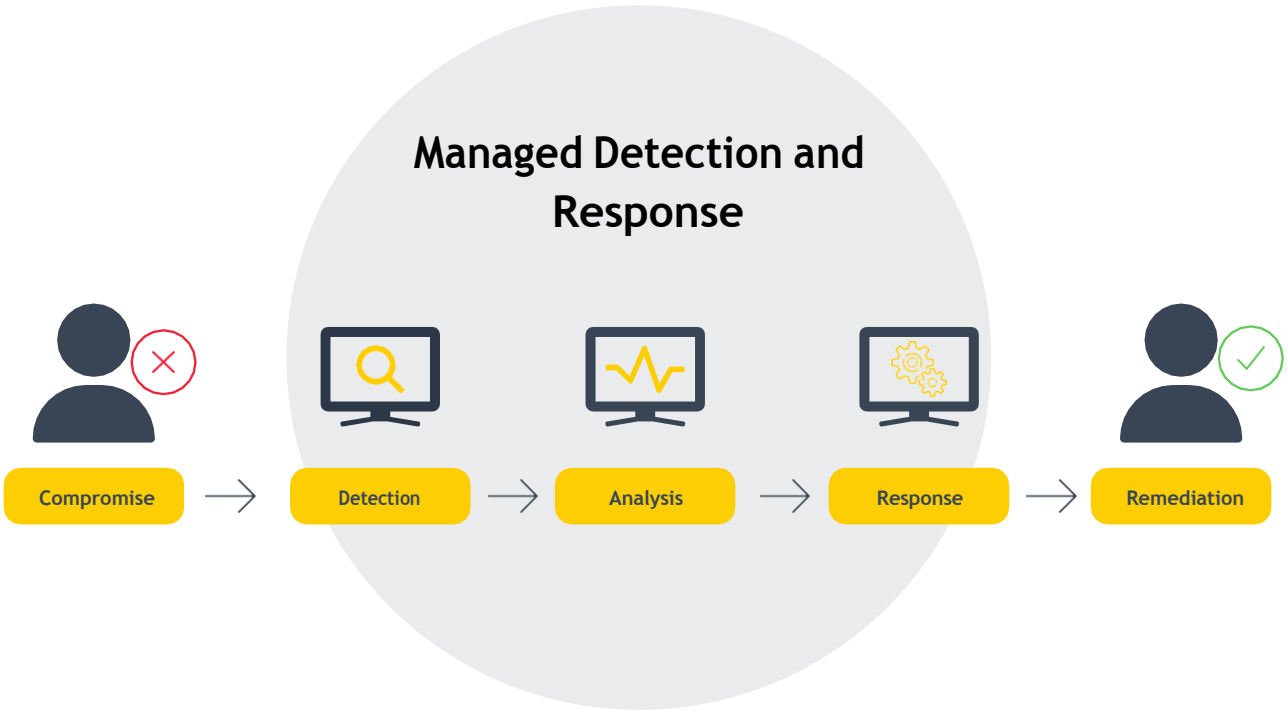
Enrichment: Additional insights during data collection and processing, SOCGUARD solutions help in integrating external threat intelli- gence to perform internal contextual lookupsor run processes to gather further data rendering to defined actions.

Orchestration: Arranging tasks to optimize a structured workflow by gathering information from a different source and consolidating it. SOCGUARD solutions integrate different security tools and platforms so they can work together.Technology integrations are the best and mostcommon method used to support technology orchestration.

Automation: This concept enables software to complete a single task or function without human involvement. Automation is not an alternative for human analysts. Instead, it reduces the analyst's time spend on simple, repetitive tasks.

Instead of wasting time on tedious manual tasks and investigating false positives, members of SOC (Security Operations Center) team can utilize their expertise to respond to events quickly and effectively.

Response: Manual or automated response provides canned resolution to programmatically defined activities. SOCGUARD automates repetitive tasks, prioritizes critical events and streamlines security processes to decrease response times drastically.

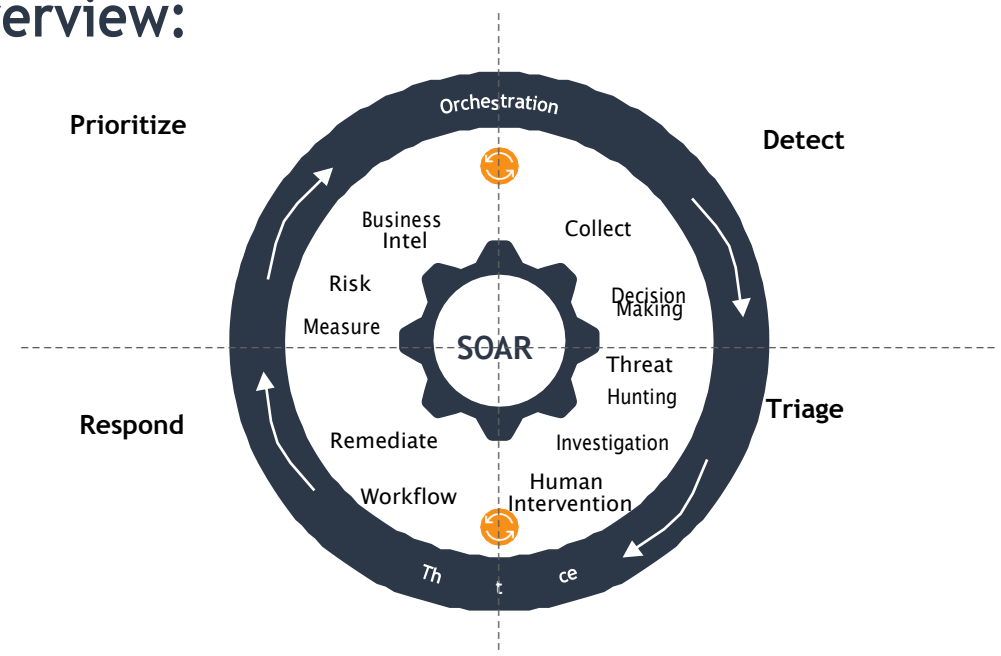


SOCGUARD benefits for delivering MDR services.

SOCGUARD's ability to orchestrate and automate are actions taken by security products without any need of human intervention. This is one of its greatest strength that allows SOCGUARD to integrate with any security process or tool that is already in use thatcan enhance the performance to add usefulness to each product.

To address scalability problems, SOCGUARD is integrated with existing security technologies.	The integration of SOCGUARD improves the abilityof MSSP's to detect and neutralize threats and attacks.
To unify asset databases, help-desk systems, configuration management systems, and other IT management tools it acts as a single "pane of glass".	SOCGUARD accelerates responsiveness to alerts triggered by arming MSSP's with the visibility and ability to react decisively to new threats or attacks such as SOCGUARD automated workflow spans for threat intelligence through the case and ticket management and provide risk and relevance between alerts.
MSSP's excess an ample amount of time dealing with false positives, because there are a greater number of alerts every day. SOCGUARD can automate the handling of such alerts, which helps analysts to focus on where decisions are needed.	SOCGUARD automates manual work of the analystto validate the legitimacy of the alerts such as new users found in the infrastructure or removing and updating rules and thus reduces the time consumption.

SOCGUARD overview:



Managed Detection and Response (MDR) security delivery service providers face many challenges in terms of both technical and human-related issues due to advanced security threats.

The solution that relies on static signature and pattern matching is incapable of detecting and responding to today's advanced security threats. Hence, many MSSP's (Managed Security Service Providers) are going behind SOCGUARD solution to improve theirdetection and response capabilities.

Developments in SOCGUARD

SOCGUARD is an Orchestrion, automation and responding system which can be developed in all its 3 Layers from the stage of data injection to the stage of response accusation, SOCGUARD platform can expand the capabilities of their software with technologies like machine learning. Machine learning complements existing SOCGUARD functionality by giving the software the means to adapt to changes in the environment. SOCGUARD platforms can learn what is and isn't normal for automation instead of relying onstatic threshold-based rules. Once these baselines are established, software updates them periodically as and when the environment changes, increasing its accuracy and reducing the number of false positives.

SOCGUARD has seen significant improvements which include process orchestration, automation of tasks or workflows. This helps in data completeness and providing a better context for alerts which reduce the amount of manual work necessary to remediate threats. Also using SOCGUARD the security team members who are not comfortable with scripting languages can use graphical playbook creation tools, while with advanced scripting knowledge retain the ability to write scripts by hand.

Critical Components of SOCGUARD Technology:

When evaluating different SOCGUARD platforms, each component should be considered as itplays an important role in the function.

01 **Customizability and Flexibility:** An effective SOCGUARD solution should be capable enough of being the single tool on top of the security stack. It should be enabled to implement in a manner that is optimized for CSIRT teams, as well as SOC's, MSSP's and security teams. Data input from a different source, including machine to machine, email, user submissions, and manual input should be supported.

In every SOCGUARD solution there will be few default integrations readily available but not all the organization's security products support, for that reason SOCGUARD solution should be flexible enough to create
bi-directional integrations with security and analytics platforms as per the customer's requirement.

02

Process Workflows: One of the key benefits of a SOCGUARD solution is its capability of automation and orchestration of processes workflows to achieve force multiplication and reduce the burden of repetitive tasks performed by analysts day-to-day. The process workflows implementation should be flexible enough to support almost any process which may need to be codified within the solution. Workflows should support the use of both custom and built-in integrations, as well as the manual task creations which to be completed by an analyst.

03

Incident Management: Orchestration and automation of security products provide clear value to any security program. SOCGUARD solution should include additional features to manage the entire IR lifecycle and to maximize the time and monetary investment. This should include case management which involves collecting, distributing and analyzing data tied to specific security incidents, to allow teams to effectively respond. A SOCGUARD platform helps organizations to reduce the meantime to detect and mean time to respond by enabling alerts to be qualified and remediated in minutes ratherthan days and weeks.

04

Threat intelligence: Threat intelligence is a critical component in effective and efficient incident response. These technologies support the vulnerability remediation. Threat intelligence must go above and beyond modest feeds to be truly effective in today's threat landscape, as a SOCGUARDsolution has access to not only the indicators but also to the incident information which can provide the added context, it is in an inimitable position to gather actionable threat intelligence.

05

Collaboration and Information Sharing: Incident response to a security alert is an equal potential responsibility of an individuals in an organization similarly SOCGUARD solution need to support collaboration and information sharing among team members in a controlled manner.

SOCGUARD Applications:

01

Proactive threat hunting: Since threat hunting usually requires analysts to rapidly coordinate among multiple security tools, it presents a great opportunity for orchestration with immediate impact. SOCGUARD tools can enable security teams to ingest third-party threat feeds and automate 'search and destroy' workflows that scan for potential vulnerabilities across environments.

02

Standardize and iterate incident processes: Security teams need to minimize 'quality variance' in incident management and response. SOCGUARD workflows are a great first step in this direction, allowing for partial/full codification of best-practice processes and guaranteeing that security analysts don't have to start from scratch each time they encounter a specific incident. With deployment maturity, SOCGUARD tools will also allow teams to quickly iterate upon these processes by spotting gaps and areasfor improvement.

03

Improve investigation quality: Multiple data points in this report suggest that security teams struggle with gathering incident context and leveraging full visibility of data at their clearance. SOCGUARD tools can help improve investigation quality by enabling faster resolution of false positives, prioritizing incidents and risk through correlated information from multiple tools and freeing up analyst time by obviating the need to learn the detailed vernacular of many security products.

04

Accelerate and scale incident response: SOCGUARD offers coordinated automation to an industry that is currently affected by important but repeatable, high-quantity tasks. SOCGUARD tools allow SOC's to rely on automation for the grunt-work and leverage rich, correlated information for decision-making and investigation.

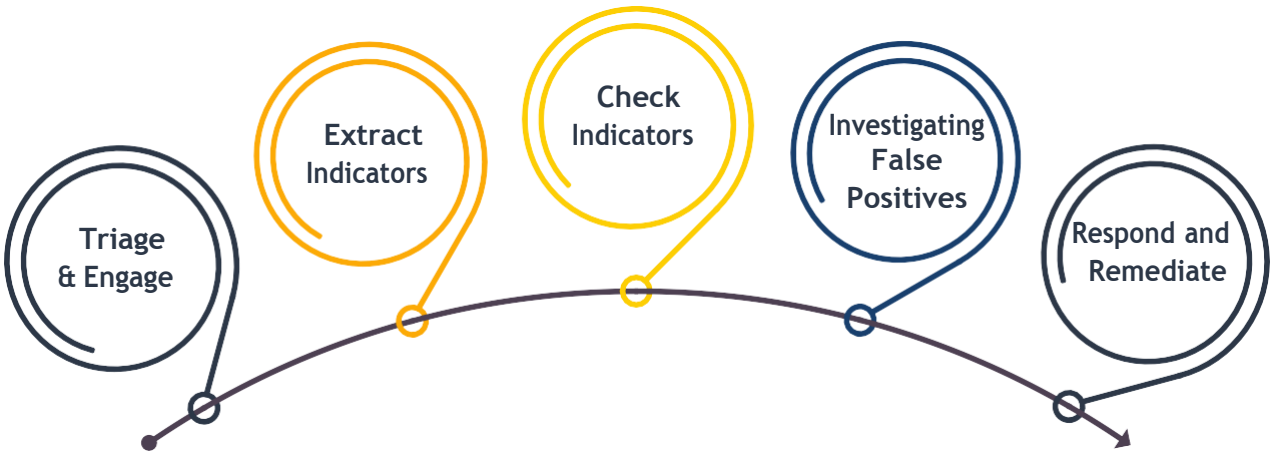
05

Security operations and maintenance: In addition to automating repetitive tasks, SOCGUARD tools can also help security teams simplify system checks, maintenance, upgrades, and general security operations. These practices rely on workflows as much as response, and standardization are needed. Automated execution will increase accuracy and better plug gaps that leavesystems vulnerable.

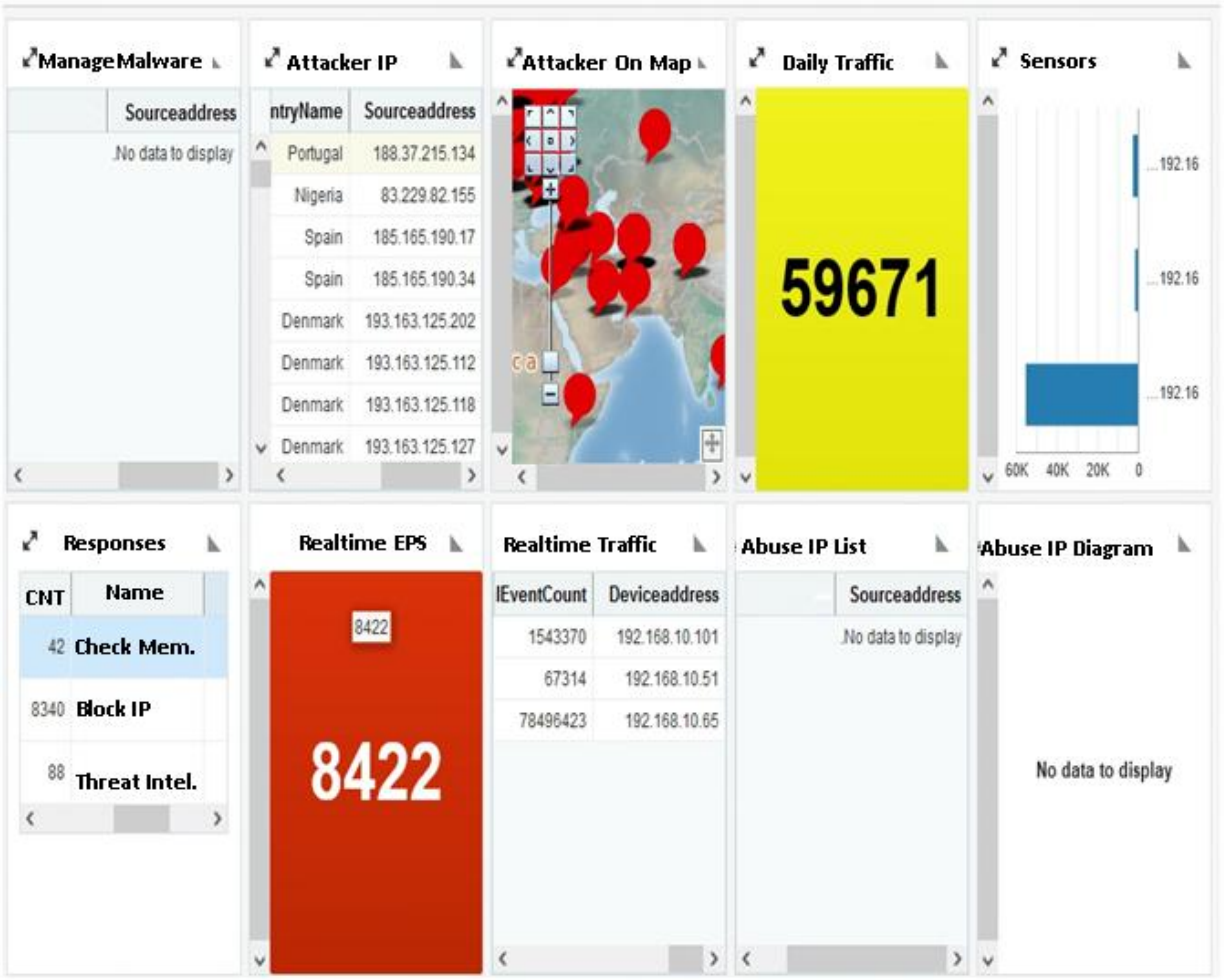
SOCGUARD Use Cases:

Use cases for SOCGUARD will vary depending on the environment and are limited only bythe creativity of the organization architecture.

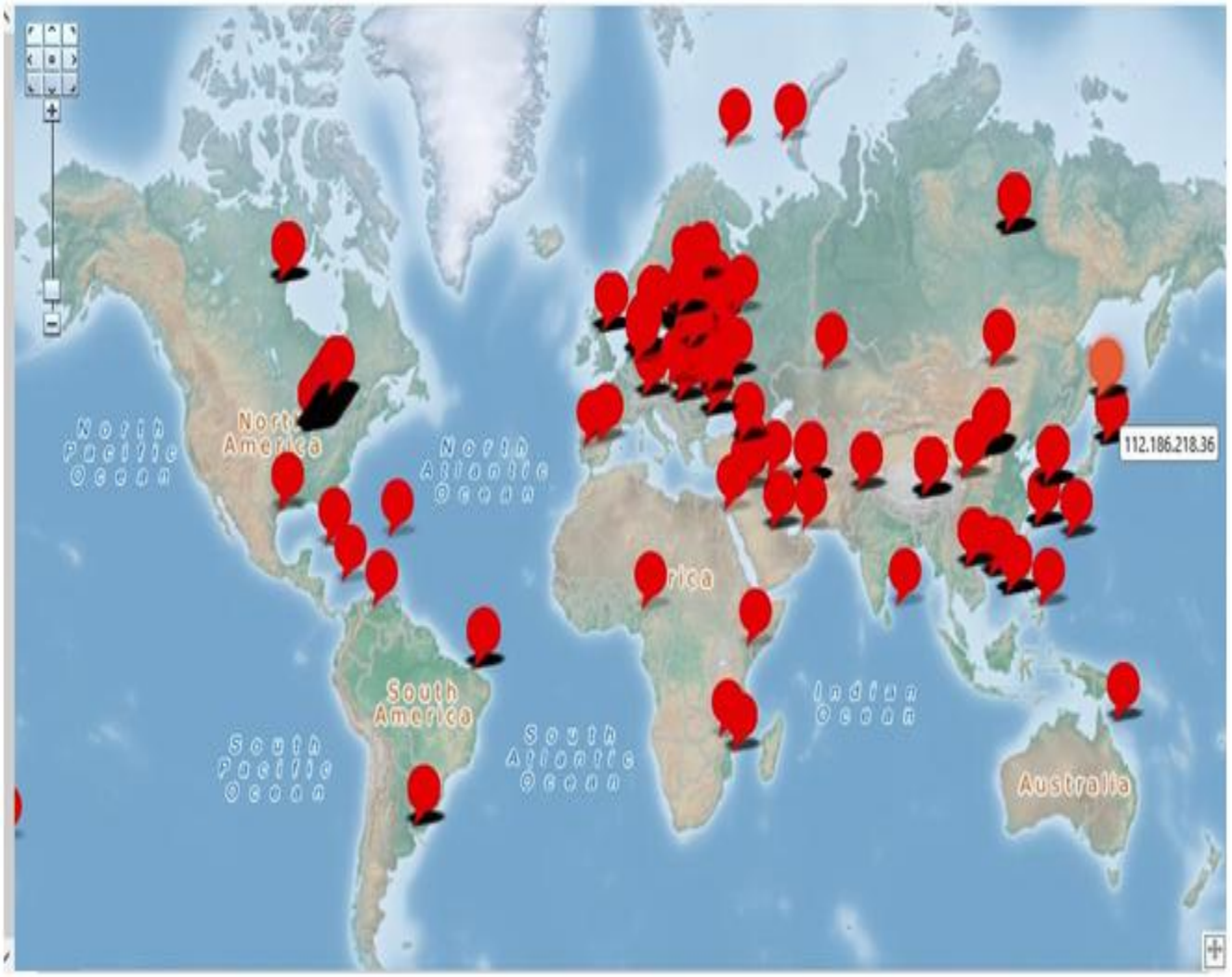
Here is the workflow that we can defne:



management report:



Attacker On Map Report



SOAR Products Compare :

SocGuard	QRadar	Arcsight	Splunk	SOLAR WINDS	Product/Indicator
OK	OK	OK	OK	OK	USE CASE
MOSTLY	400+	400+	MOSTLY	-	Data source
1000000	1000000	100000	PETABYTE DAILY	25M PER DAY	MAX EPS
MACHINE LEARNING AND UEBA AND FORENSICS	MACHINE LEARNING AND UEBA AND FORENSICS	MACHINE LEARNING	MACHINE LEARNING AND UEBA	ABNORMAL BEHAVIOR	INTELLIGENCE
SOFTWARE OR CLOUD	APPLIANCE OR SOFTWARE OR CLOUD	APPLIANCE OR SOFTWARE OR CLOUD	SOFTWARE OR CLOUD	VIRTUAL APPLIANCE	DELIVERY
SC,UF,Syslog,CUSTOM	Wincollect,Syslog	SC,Syslog	UF	SEM	Support Agent
BASE ON MAX DAILY DATA OR EPS	PER MONTH	BASE ON MAX DAILY DATA OR EPS	BASE ON MAX DAILY DATA GB/DAY	PER NODES	PRICING

Contact us

Sales Manager:

Mr.KARIMI
+989219427704
info@socguard.ir