Infopercept

Security Orchestration, Automation And Response

Infopercept

Why SOAR ?

Difficulties faced without automation:

- Face increasingly hostile threat landscape
- Rely on manual, document-based producers for operations.
- Have longer analyst onboarding times.
- Lack people, expertise and budgets to protect against threats adequately.
- Escalating volume of Alerts
- Multiple static consoles / Vendors used for investigation
- Need of improvement in speed of detection
- Rising cost due to all of the above

How can SOAR help ?

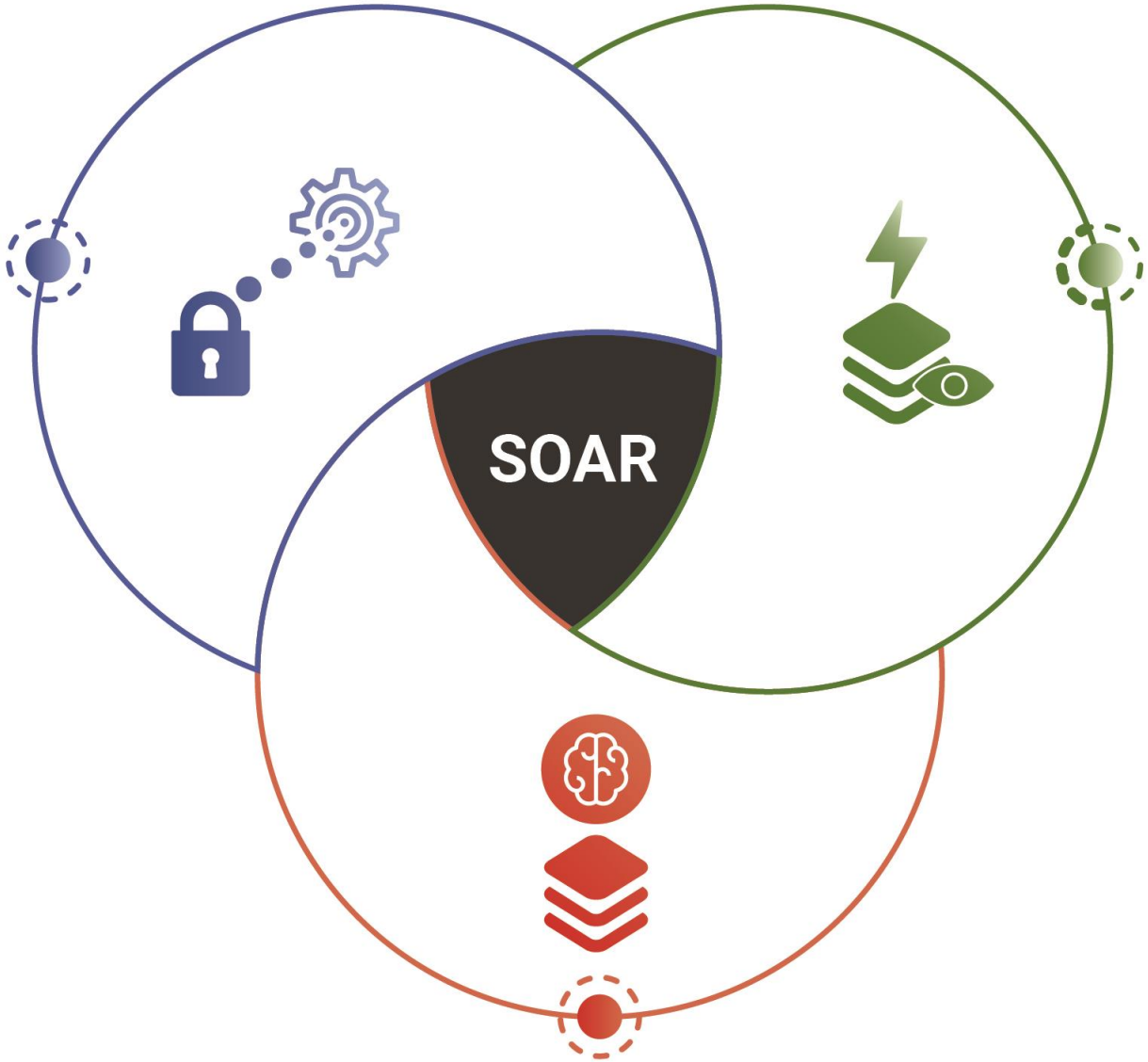
- A good SOAR can help you compile automation playbooks to alleviate some of those important, but time-consuming, manual tasks and manage complex use cases.
- Security products are being designed with extensive API capabilities.
- More cloud based events providing context to events like reputation services , sandbox , threat intelligence , feeds , etc.
- Uplift in development operations capability in the industry driving IT Automation.
- Python and other robust programming languages.

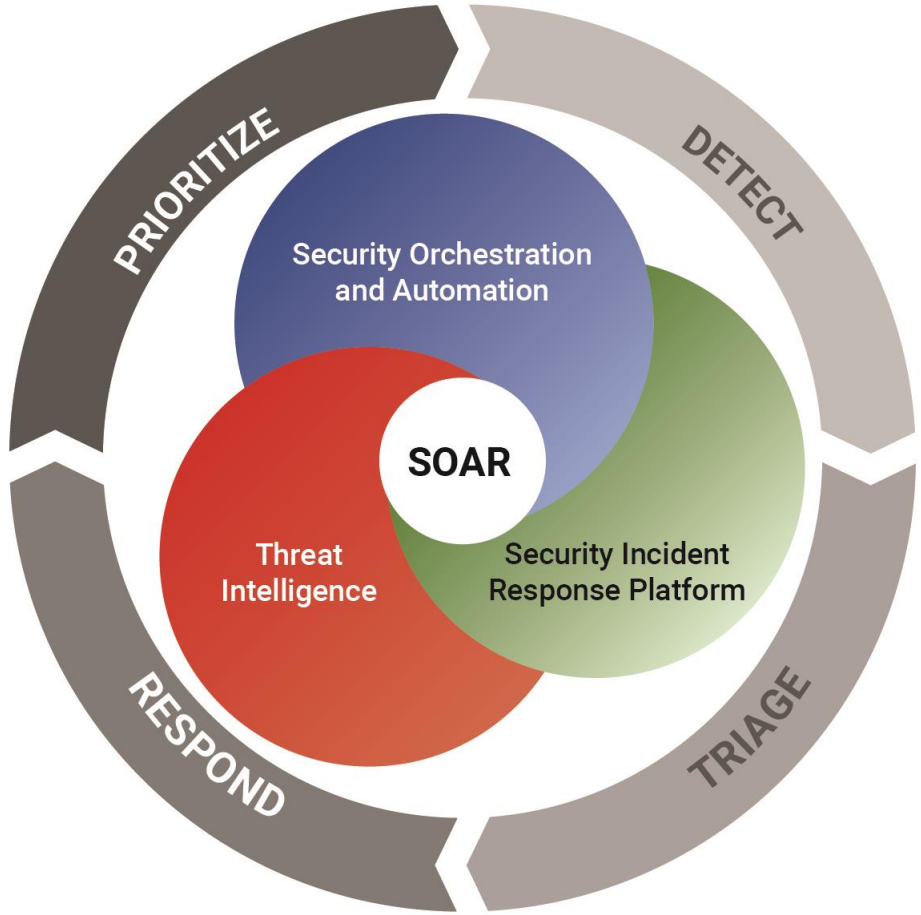
Infopercept

SOAR : Its full form is “Security Orchestration, Automation and Response.”

- It aims to provide a solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance.

- It can be applied to compatible products and services that help define, prioritize, standardize and automate incident response functions.


SOAR


PRIORITIZE
DETECT
TRIAGE
RESPOND
Security Orchestration and Automation
SOAR
Threat Intelligence
Security Incident Response Platform

What is SOAR ?

Security orchestration

It is all about gathering information from a variety of sources and consolidating it in a useful way

Automation

Security automation refers to features that enable software to take action without human intervention. Automation isn’t a replacement for human analysts; instead, it reduces the time analysts spend on simple, repetitive tasks. This lets them spend more time focusing on more complex matters where their attention and expertise are genuinely needed.

Response

Reporting , collaboration and case management. Policy based coordination of human and machine based activities for event/case/incident workflow

Infopercept

Features of SOAR

Threat and vulnerability management:

These technologies support the remediation of vulnerabilities. They provide formalized workflow, reporting and collaboration capabilities.

Security incident response:

These technologies support how an organization plans, manages, tracks and coordinates the response to a security incident. Security operations automation:

Security operations automation:

These technologies support the automation and orchestration of workflows, processes, policy execution and reporting.

Respond to incidents

Sets of rules called playbooks enable SOAR platforms to take action automatically when a particular kind of incident occurs. Using this functionality, you can set up automated responses for the most common incident types.

Manage Vulnerabilities

Correlate log data with threat intelligence to understand what exploits attackers are using, and identify vulnerable elements of your infrastructure before they can be compromised

Coordinate Investigation

Organize security data easily and retrieve relevant third-party threat intelligence when you need it. Instant access to external data sources helps your analysts make the right decision in every investigation.

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. SOAR helps you eliminate these barriers to collaboration.

“You can’t build an orchestra with a single Wood Instrument. “

As mentioned above SOAR has many tasks associated with it in order to provide complete functioning of SOAR as automation they are as follows :

- Case management
- Automation and orchestration
- Threat Intelligence Management
- Workflow Engine
- Checklist for complete SOAR solution can be found by CHECKLIST

Infopercept

Case and threat intelligence management

Case management

A fully-capable SOAR platform maintains all information and enriched data gathered from automated and orchestrated activities and can provide a detailed audit log of all actions taken during the response.

Threat Intelligence Management

Threat intelligence is organized, analyzed and refined information about potential or current attacks that threaten an organization

A good SOAR platform can access multiple feeds to add enrichment and maintain a view of the threat landscape.

Infopercept

Automation, orchestration and Workflow Engine

Automation

Setting up a single task to run on its own – automating one thing . This single task can be anything from launching a web server, stopping a service, etc. or automating the creation of workflow

Orchestration

Automatically execute a larger workflow or process comprising of manual and automated steps.

Workflow

It is a part of SOAR but if it's the only element required, then a fully-capable SOAR platform is not required.

Infopercept

Playbooks

Orchestration playbooks can be built to be more adaptive to changing adversary capabilities, attack patterns, and infrastructure as both internal and external threat intelligence is available. In some cases, threat intelligence allows the process to automatically adjust itself and helps you drive further decision-making.

It is a playbook definition that makes use of ecosystem orchestration. Machine based execution and decision making workflow (with and without human interaction)

Infopercept

Use Case 1 : Phishing Attack

Application of SOAR

Issues :

- Huge attack volume and velocity
- SOCs and analysts can’t keep up
- Switching multiple screens to coordinate responses
- Unable to standardize response and reporting
- Photo of phishing attack

How can it be overcome by using SOAR:

- Trigger phishing playbooks to run repeatable tasks at machine speed
- Identify false positives and standardized SOC responses at scale
- Extract header information, email addresses, URLs and even attachments Automate submission of data to threat intelligence services
- Conduct detailed scan of network logs
- Contain malicious threats
- Delete phishing instances, block IP or URLs, ban executables.
- Reduce investigation time from hours to minutes

Infopercept

Use case 2 : Malicious network traffic

Application of SOAR

Issues :

- Generates many alerts deemed malicious by detection technology
- Creates false positives or low priority alerts
- Often left in queue awaiting investigation
- Security teams have little or no capacity to conduct triage

Method to overcome :

- Apply automatic data enrichment tools
- Search additional threat instances via automated workflows
- Immediate triage and response upon threat alert
- Auto trigger of containment by blocking IP or isolating host

Infopercept

Use case 3 : Vulnerability management

Application of SOAR

Issues :

- Reviews and alerts system owners to potential weakness \Time-consuming but critical task
- Often performed externally
- Carriers risk of undetected threats within IT infrastructure

Method to overcome :

- Improve dynamic threat analysis by automating workflows
- Boosts productivity of security analysts
- Dramatically increase ability to detect sophisticated threats

Infopercept

Use case 4 : Processing data logs

Application of SOAR

Issues :

- Too much data to organize manually and accurately for decision making
- Log entry volumes are too high for threat detection and response
- Cumbersome to process log data into right format for remediation

Method to overcome :

- Correlate the data independently
- Pull in all threat data across the network
- Validate against external threat intelligence sources
- Help analysts identify threats and decide on next steps

Infopercept

Use case 5 : Improving lines of communication

Application of SOAR

Issues :

- Security teams frequently fail to update key stakeholders about potential threats
- They are too busy to send out information
- Clunky messaging platforms are challenging to use and deter communication

Method to overcome :

- Free up security staff resources to focus on more important tasks
- Develop better metrics for response times from different departments
- Increase the security team’s voice with company executives

Infopercept

Use case 6 : Dwell times

Application of SOAR

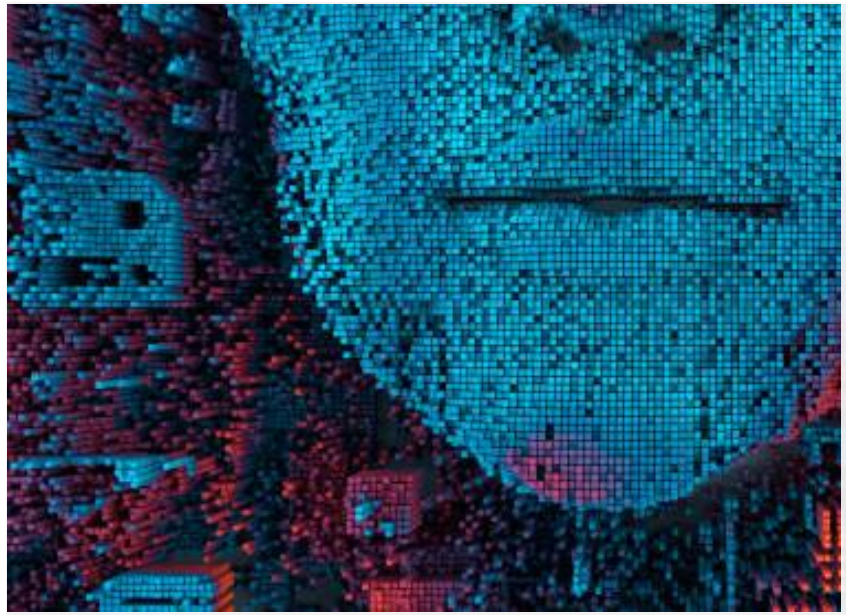
Issues :

- Manual correlation and analysis of data
- Laborious data collation across end points, servers and mobile devices
- Difficult to scale tasks and workflows
- Average dwell time to detect and contain intruder : 50 to 150 days

Method to overcome :

- Accelerate investigation and detection
- Improve accuracy of analysis
- Increase remediation success rates
- Reduce dwell times to hours

Infopercept



Use case 7 : Mitigating threats faster than they spread

Application of SOAR

Issues :

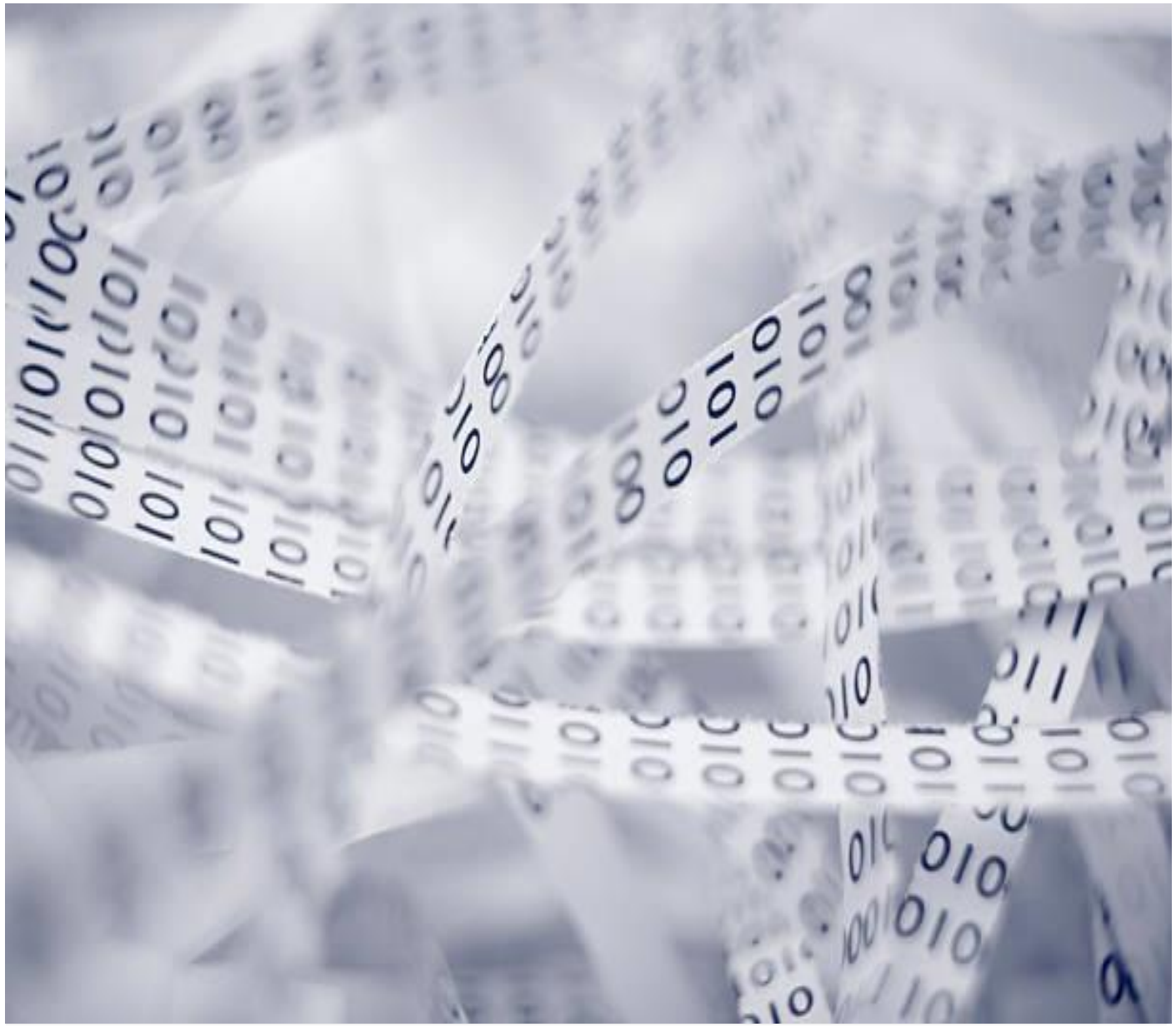
- Difficult to protect against fast moving threats
- Challenging to deploy sets of protection using different technologies
- Time-consuming, manual task.
- Involves multiple security vendors in the technology stack

Method to overcome :

- Speed up responses times
- Enable protections on the fly
- Eliminate additional strain on SOC resources
- Aggregate and validate data from a wide range of security products

Infopercept

Importance of SOAR in banking industry



- Now a days automation is essential factor.
- Also bank is going digitized.
- So net banking plays an important role in digital world.
- Hence threats related to net banking is also increasing drastically.
- In order to overcome one can go for secure integration of bank with automation in order to reduce human efforts and use resources efficiently.
- For this, we firstly need to know what are the threats present in banking.

Infopercept

Threats in banking

There are numerous types of banking threats present which are listed below :

- Carding fraud
- Paypal (Paypai)
- Accounting fraud
- Cheque kiting
- Fraudulent loan applications
- Payment card fraud

Details

Carding Frauds:

- **Issue :** Unknowingly storage of card details in cookies and cache memory
- **Overcome** : Design a playbook such that it deletes these data as soon as the client leaves the page or log out from the page.

Accounting fraud:

- **Issue :** In order to hide serious financial problems, some businesses have been known to use fraudulent bookkeeping to overstate sales and income, inflate the worth of the company's assets, or state a profit when the company is operating at a loss.
- **Overcome** : using playbook one can check the actual identity of the client using their personal data which is.

Paypal (Paypai) :

- **Issue :** It is a phishing scam, which targets account holders of the widely used internet payment service, PayPal, taking advantage of the fact that a capital "i" may be difficult to distinguish from a lower-case "L" in some computer fonts. This is a form of a homograph attack.
- **Overcome :** One can design a playbook which when implemented will scan the web address requested by the client along with the details like name , IP address, etc. and compare it with actual site databases if it matches the client’s details then client gets access but if not then it will automatically block the IP address.

Conclusion

- Although SIEM correlation rules consolidate events into a single alert, the SOC team still needs to explore each endpoint to get more information about the incident.
- Once the attack is revealed, the security team needs to access the FTP servers and check the firewall log, the DLP system status and the Event of the targeted servers and more.
- Addressing this challenge with one intelligent, easy-to-use environment for all security operations is provided by many tools like Simplify Nexus, ArcSight, LogRhythm, etc.

- Advance technology provides more security and facility to us, so it is important to understand and make efficient use of these technologies.
- Here we ultimately goal to automate few banking tasks in order to reduce unnecessary wastage of human resources and time by automating this tasks using scripting.
- Playbooks are designed to automate those works which are of less concern and in contrary one can invest this time to solve problems where human assistance is actually needed.

Infopercept

THANK YOU

For More Information Please Visit our Website

www.infopercept.com