InquisIT

Security Orchestration Automation and Response (SOAR)

InquisIT, LLC.
14900 Bogle Drive, Suite 203
Chantilly, VA 20151

Info@inquisitllc.com
www.inquisitllc.com

Incident Response: A 3-Fold Problem

Currently, inside of all organizations, either large or small, the issue of performing incident response is an enormous task to tackle since ***most organizations are now struggling to try to find candidates that have real-world experience in the online battlegrounds.*** This is in part due to the many factors of Cyber Security Incident Response. With the primary factor being in the world of information technology, overall cybersecurity is still a relatively new field. It is thus causing employers to look for incident responders that may not have the amount of seasoned experience required to deal with the onslaught of attacks and breaches that occur daily. From the smallest of attacks (for example, a user getting a tracking cookie) to the most significant full-scale data breaches in the latest news. The task of finding a cybersecurity professional in the small pool of candidates seems to be getting harder and harder every day, while attacks from both outsiders and insider threats are ever-growing.

In addition to the issue of finding incident handlers while an on-going onslaught of attackers threatens your networks, many organizations that already currently have ***Cybersecurity professionals on staff are struggling to keep up.*** This is due in part to diminishing budgets, hiring freezes, or the fact that the legacy methods of working incidents is too slow-paced. The latter is witnessed in reviewing working times for incidents, even those that can be considered small, such as a reported phishing attack, cause an incident handler to waste at least 45 minutes investigating, responding, and blocking the attackers thoroughly. Even worse are the larger-scale attacks occupying incident responders for multiple days of data searching, interviewing, and responding to help remediate the attack.

Lastly, another resulting issue raised from overworked and understaffed incident response individuals is that due to lack of time and employee work-force, ***not all incidents get reviewed as precisely as required.*** As a result, a simple step that the response individual may have overlooked while trying to handle another pressing case, leaves the original vulnerability un-remediated and still open for other attackers around the globe.

CYBERSECURITY PROFESSIONALS STRUGGLE TO KEEP UP
NOT ALL INCIDENTS REVIEWED AS PRECISELY AS REQUIRED

What Is Information Security Orchestration, Automation, And Response (SOAR)?

Information Security Orchestration, Automation, and Response (SOAR) works just as an orchestrator works within an orchestra, but instead of controlling and conducting multiple individuals playing different varying instruments, ***SOAR manipulates numerous diverse tools to create a more streamlined and fluent process for incident response***.

Unlike a general Orchestrator, SOAR does not utilize just individuals; instead SOAR utilizes security tools, security policies, and people to create a better flow of processes. Most practically, SOAR creates automated and quicker manual actions to save overworked and understaffed security teams valuable time to focus on the more severe incidents.

In more technical terms, this is accomplished through integrations of tools via API's. For instance, by connecting an API to a Security Information and Event Management platform (SIEM), responders would be able to automatically perform data calls upon the SIEM's database to pull the latest security logs and artifact information. Thus, saving the incident handlers valuable time in searching and creating automated remediation tactics based on the pulled information. These remediation tactics could be as simple as a button that automatically generates an email to an individual phished, informing the victim that they should remove the phishing email; or a tactic as detailed as integrations into their firewall to completely shut off communication going to or from specific IP addresses and ranges.

Investigation
Case Creation
Collaboration
Threat Detection
Mitigation & Response
SOAR

How Can SOAR Help An Underpopulated And Overworked Work-Force?

SOAR will help alleviate many issues that arise from complications of legacy incident response techniques as discussed in the introduction through multiple advancements provided from Orchestration. Several of these new-age advancements include:

Automation Of Log Data Ingestion: With automation of log ingestion into a SOAR, the issue of searching and combing through endless upon endless security event logs to find the needle in the haystack is alleviated. These configurations are accomplished through a combination of scripting and API connections between the devices to identify the information to be pulled correctly.

Prioritization of Incidents: Through the use of prioritization of incidents, both management and incident handlers can quickly review attacks and rank them based on severity, impact, efficacy, and several other paratmeters. This would allow incident handlers to focus more of their time and efforts on addressing the more severe attacks on-going within the network.

Automated Threat Data Ingestion Through Feeds: Via the use of integrated threat feeds, security handlers can review threat information on the ingested artifacts sent into the SOAR tool automatically. Thus, alleviating the issue of taking critical pieces of information, for example, IP addresses, file hashes, or any other indicator of comprise(IOCs), and inputting them into an online evaluation tool to obtain accurate threat data.

Playbooks To Keep Everyone On The Same Working Page: Utilizing playbooks, incident handlers can convert their current multi-page handbooks and policy guides into quick, learn-as-you-work methods. In turn, this would allow all incident handlers to work based on up-to-date guidelines, utilizing the appropriate tactics from either industry best-practices or in-house techniques, in addition to keeping all incident handlers on the same page. Through the use of playbooks, even the most novice security professionals can work at peak performance and follow organization standards to respond to incidents, both large and small.

Automated Activities: From automated activities and integrations inside of SOAR tools, incident handlers can accomplish remediation tasks in a matter of seconds that previously would have taken up to 30 minutes to complete. SOAR provides incident handlers the ability to complete lower priority incidents quicker in order to focus on the more severe attacks. Along with creating a quicker time to resolution, automated actions accomplished by SOAR tools allow all activities that are utilized for remediation to become standardized. For example, instead of sending multiple different instructions to the local onsite technical support, through the use of automation, all instructions, attachments, and language are standardized prior to sending to alleviate any confusion.

How Will This Help?

Utilizing the several methods listed above along with multiple other out-of-the-box integrations that are part of any SOAR platform, SOAR tools can alleviate most issues that occur inside of incident response teams every day across all organizations. Some of the ways SOAR alleviates these issues inclues:

Quicker Time To Resolutions For Incidents. Through the removal of the most mundane and time-consuming actions performed by incident handlers, SOAR shortens resolution time from days and weeks down to minutes and hours. Configurations accomplished through bidirectional integrations into all security tools provide real-time content updates that incident handlers utilize every day automatically.

Broadening The Work-Force Pool And Creating More Natural Training For Incident Response. From the use of playbooks integrated into SOAR tools, management now has an easier time finding and training new incident handlers for their organizations. Since all organizations are unique, playbooks help to point incident handlers into the right direction quicker. Playbooks train incident handlers on how to respond to incidents in real time during the time allotted for resolution, instead of the older ways where the responder would have to read standard operating procedure document after document.

Better Value Out Of Incident Response. Organizations receive better value from their incident response teams by leveraging the following benefits that come from utilizing a SOAR tool:

- Quicker time to resolutions from automation and limiting of mundane everyday tasks
- Prioritization of incidents through ingested live threat data and scoring algorithms
- Full tracking of tasks through timers and reporting
- Playbooks to create ease of use for incident handlers utilizing multiple tools

USE CASES

1 Automatically blocking IP addresses of threat actors through simple clicks.

In this first use case, let us assume that your organization is under attack from an outside threat actor performing SQL injections against a web application hosted inside your agency. Through the use of your SOAR tool, alerts are automatically generated into the device and create a new incident for your responders to investigate. The on-call incident handler logs into the SOAR tool and based on the automatically ingested threat feeds, realizes that the main source IP address is incoming from a known international advanced persistent threat group. After a quick review of the automatically ingested logs from your SIEM, the incident responder realizes that this same source IP is attacking multiple servers. Concluding the investigation phase, the incident responder has decided that this attack is valid and of high priority. The incident handler requests and receives immediate approval to shut down the source IP inside of the boundary firewall. Through a quick click of a button, the incident handler has now added the source IP into the inbound blocking policy set and effectively cuts off this attack at the source. With the use of your newly implemented SOAR tool, your security incident handler has just removed an APT from attacking the network in a matter of minutes, versus the older methods taking several hours of investigation to understand the bigger picture.

2 Removal and remediation of an infected machine.

In the second scenario, one of your internal users accidentally clicks on a link sent in a phishing email that has now installed the latest ransomware on the user's machine. This ransomware is triggering alerts on the local SIEM that is now automatically ingested into the new SOAR tool. Through the constant bidirectional feeds, you realize this malware is encrypting more and more files on the victim's machine. Through quick actions, the incident handler quickly creates a support ticket to the local onsite technician to have the device removed from the network before it has a chance to spread and affect multiple other machines on the same segment. Through the utilization of the SOAR tool, the incident handler has successfully removed the infected computer to be remediated in a matter of minutes since the manual task has now become automated, allowing responders to skip time-consuming steps. The previous way of manually addressing the incident would have been as follows: 1) investigate the issue, 2) realize that the ransomware is more severe than first expected, and 3) manuall create the ticket and input all instructions to the local help desk. When combined, all of these skipped steps have prevented a potential network-wide ransomware attack, thus, saving the organization multiple hours and costly recovery steps that could have caused severe impact to the business.

Conclusion

Utilizing many of the key features inside of Information Security Orchestration, Automation, and Response (SOAR) tools, including automation, integration, and playbooks, organizations can accomplish and conquer all complications that occur with the limited work-force pool of security professional across the industry today.

Along with helping organizations get a better value out of their incident handling team, SOAR reduces incident resolution time from weeks or months, down to minutes or hours after the initial alerting.

Overall, SOAR tools help create the highest functioning and most successful incident response teams that can be available to any organization.

About InquisIT, LLC

InquisIT is an information technology contracting organization that has experience working with large scale agencies encountering issues concerning cybersecurity and coaching them into the latest bleeding-edge support to help further the progression of Technology while providing better-than-best industry practices.

InquisIT conquers these challenges through its vast experience implementing multiple Information Security, Orchestration, Automation, and Response (SOAR) tools, alongside integrating the systems that are required to streamline incident response.