Automating Security Operations

for Mid-Enterprise

graylog

Why Mid-Enterprise Organizations Need to Automate Their Security Operations

At the end of January 2023, ION Cleared Derivatives, a division of ION Markets, was the victim of a ransomware attack that took systems that help automate the trading lifecycle of financial companies offline. As a result of the attack, all ION customers in the finance space had to manually confirm their trades, estimate commodity prices, and revise them later in an effort to mitigate lengthy delays in reporting. LockBit claimed responsibility for the attack and threatened to leak the stolen data in February unless their ransom demand was met. After root cause efforts, ION stated the incident was isolated to a small number of smaller and mid-size firms.

Automating Security Operations: Benefits and ROI

When your data is threatened, time is of the essence. Even a few minutes may make the difference between a duly mitigated threat and a real catastrophe, especially when so much as private or financial information is at stake. Skilled security professionals do not come cheap. When the average U.S. mid-enterprise deals with hundreds, and sometimes even thousands, of security alerts per day, it's easy to see how numbers can quickly add up and cause costs to hit the fan in no time.

Automation can dramatically improve response efforts, reducing average time to respond to most threats from hours to minutes, saving incalculable amounts of time. But automation doesn't simply provide value in terms of working hours or efficiency in mitigating damage (which are worth millions already). Dealing with so many security events each day often causes mid-enterprise security analysts and SecOps teams to suffer from alert fatigue. This means that each employee's ability to stave off a threat is lowered, while automation dramatically improves their accuracy and helps them do more with the resources they have.

Some of the Complicated Manual Tasks Performed by Security Analysts:

- Manually operating security tickets where all evidence should be up-to-date and tracked
- Sending countless notifications to impacted users, often working in different departments or even different geographies
- Prioritizing security alerts when the daily volume is unbearably high

Security Orchestration, Automation, and Response (SOAR)

Security Intelligence found that 43% of cyber-attacks are aimed at the mid-enterprise, but only 14% indicate they are prepared to respond. Is yours among them? Maybe. SOAR stacks (Security Orchestration, Automation and Response) are advanced security solutions composed of compatible tools that collect security data from multiple sources, sort them through, and automate their responses without human assistance

The SOAR market is expected to grow from an estimated value of USD 1.1 billion in 2022 to USD 2.3 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 15.8% from 2022 to 2027. By leveraging an incredibly effective combination of human and machine power, orchestration tools can improve the efficiency of your incident response activities, reduce the workload of your SecOps specialists, and save precious resources. In the current cyberthreat landscape, there's no reason for your most valuable talent to spend time on repetitive, manual tasks or false positives.

Which Tasks Can Be Simplified By Automated Security Operations?

- Collecting and centralizing log data
- Submitting log data to threat intelligence platforms
- Orchestrating log data across several platforms
- Submit attachments to sandbox platforms for review
- Notifying impacted users in real time
- Quarantine infected devices

The SOAR market is expected to grow from an estimated value of USD 1.1 billion in 2022 to USD 2.3 billion by 2027

Building a 360° Integrated Security Environment

SOAR stacks and SIEM/Log Management solutions are necessary— but they're just the tip of the iceberg. They can certainly automate repetitive security tasks, but that's like buying a Lamborghini just to drive it from work to home every day; there's so much more you can do with it. And there's even more you can do if you integrate them together.

Smaller security event investigative teams are learning that an orchestrating tool is just one of the weapons needed to fight off hordes of malicious software and malware attacks. No software can provide the necessary resistance against the most insidious cyberthreat if you're not able to aggregate all the data coming from a broad range of different sources. It's time to establish an impenetrable 360° integrated security environment by merging all your weapons together.

What Are the Most Common Use Cases of Automated Security?

- Smart malware analysis
- Stopping endpoint attacks
- Preventing phishing attempts
- Managing SSL certificates
- Detecting suspicious logins (repeated failures, unusual devices, remote locations)
- Hunting indicators of compromise
- Vulnerability management

Integrating Log Management Tools with Automated Security

Log management tools are the best way to efficiently and effectively deal with the massive quantities of raw log data that make up the foundation of SOAR stacks. Integrating log management into a SOAR platform is simple. Let's have a look at how centralized logging can empower any automated security system and make it even more efficient by increasing agility and operational efficiency.

Improving the Depth of Threat Analysis and Detection

The logging tool will ingest the logs and do its normal processing to convert the logs to standard format, with source/destination info, user info, and enrich it with threat intelligence, asset lists, geo-location, and other useful information. Once all this data is compiled, the correlation engine will run to create an alert in the system. This is the starting point of the integration.

The SOAR product will then query the alerts on a frequent basis to pull in any new alerts with a specified parameter (name, severity, etc.) and then kick off the workflow. When the routine is started, the logging tool can be queried for additional logs which could add new layers of depth to the automatized investigation.

The log manager can be set to collect all data from your environment into one centralized area. The SOAR stack will run through the playbook and do all its required steps before the ticket is closed. After this is done, a human analyst would see the alert in the SOAR platform, take a field in the alert (i.e., Username, IP, Hostname) and then come back into the log manager to do further investigation into the user and the actions they took. More information means that SecOps specialists have a clearer picture of the actual threat. The more they know the better the chance is to identify malicious actors, understand their behavior, perform root-cause analyses, establish prevention and remediation strategies, and pinpoint vulnerabilities.

Framing the Risk to Avoid Blocking Legitimate Communication

Automated blocking does a lot more than just saving analyst's time. The right threat intelligence feed can help you detect all logins from unusual locations or devices and block the obvious threat actors attempting to connect with your assets, systems, and network.

However, many mid-enterprise organizations are concerned that an automated threat response may hamper legitimate traffic. The remedy is setting a high bar for automated blocking. By aggregating logs, you can set multi-layer rules that will detect when an attempt is accompanied by a second alert from a different technology. Rules can define when events should be linked together before an alert is sent, so that a simple attempt from a known indicator is never blocked.

Rather than sending one event at a time, a log management correlation engine can make more educated alerts, reduce the number of false positives, and request an investigation only when a high-priority alert is configured.

Integrating Threat Intelligence

Automated security and orchestration solutions are efficient only when they can rely on a correct set of rules. Threat intelligence feeds are required to tell the machine what it is

supposed to do with the information it gets. The more detailed and reliable this information is, the more efficient the automated response will be. The right threat intelligence is vital to minimize the likelihood of misdirection and false positives.

Efficient log management means that a SOAR or SIEM won't eat up all your resources with harmless events. Logs coming into the log management system can be enriched in many ways before they are integrated into threat intelligence feeds. For example, they can be geo- tagged, allowing for the SOAR platform to quickly detect alert rules with a different country attached to it. The logging tool can also be tied to different threat intelligence feeds, adding threat telemetry to the logs that allows for better decision making in the SOAR system as well.

Examples of Integrating Log Management and SOAR:

1. Detecting a known bad IP addresses via threat intelligence so the IP address is automatically added to the block list on the firewall.

2. Detecting a brute force attack followed by an account creation event. When the threat is detected, the account will be disabled until verified by the administrator.

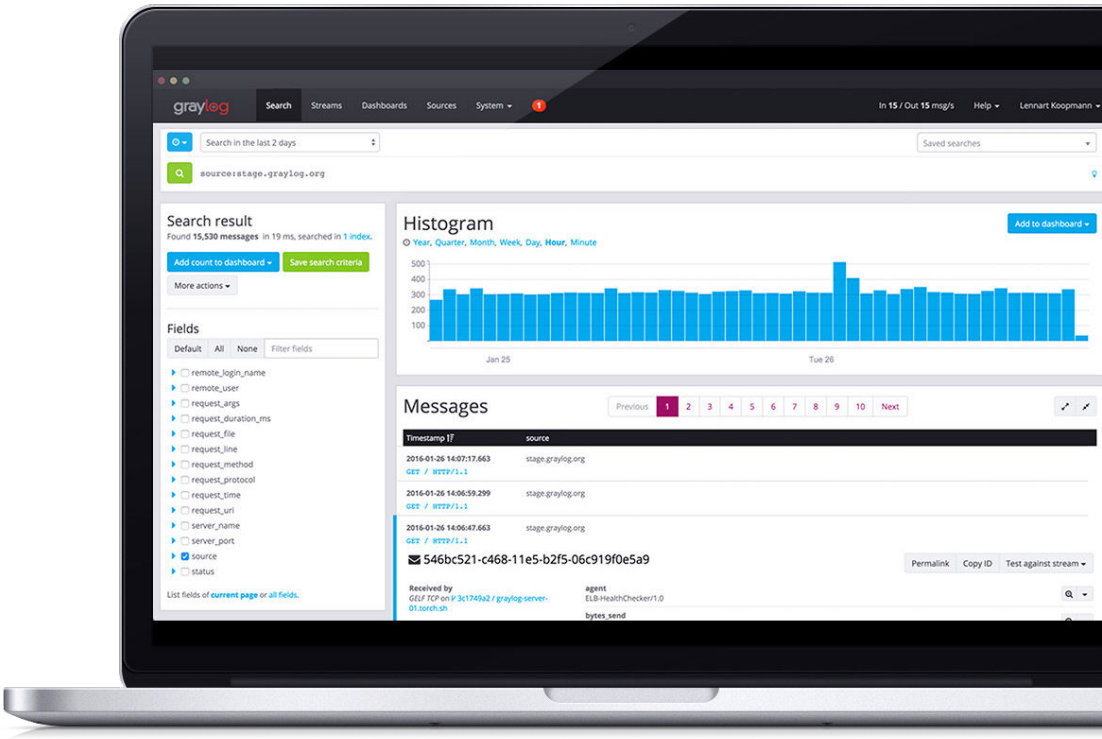
3. Detecting a known piece of malware via MD5 Hash and doing a quarantine and lockdown event on the host to possibly take the host off the network or shut it down.

Security Automation is a Necessity, Not a Luxury

The recent history of the LockBit attack taught us a very important lesson - unless we learn how to integrate automation into our mid-enterprise security solutions, we won't be able to keep up with the evolving threat landscape. When a system can infect,

harvest credentials, move laterally, and then act to wreak havoc on even the most watertight organization without the help of a single human being, fighting against it without some degree of automation is like bringing a knife to a gunfight. The LockBit attack happened in 2023. Tomorrow's cyber threats will be even more sophisticated and dangerous.

Tomorrow's cyber threats will be even more sophisticated and dangerous.



About Graylog

Graylog is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.

graylog

www.graylog.org
info@graylog.com
1301 Fannin Street, Suite 2000
Houston, TX 77002

©2024 Graylog, Inc. All rights reserved.