```
<134>Jan 11 07:28:41    07:28:41 filterlog: 5,,,1000000103,em0,mat
<134>Jan 11 07:13:47    07:13:47 filterlog: 5,,,1000000103,em0,mat
<190>Jan 11 07:41:55    07:41:55 dhcpd: DHCPREQUEST for 10.0.0.187
<134>Jan 11 07:53:22    07:53:22 filterlog: 5,,,1000000103,em0,mat
<134>Jan 11 08:02:41    08:02:41 filterlog: 5,,,1000000103,em0,mat
<134>Jan 11 08:13:47    08:02:41 filterlog: 7,,,1000000105,igb0,ma
<190>Jan 11 08:41:55    08:41:55 dhcpd: DHCPREQUEST for 10.0.0.187
```

# AUTOMATING SECURITY OPERATIONS

## WHY ORGANIZATIONS NEED TO AUTOMATE THEIR SECURITY OPERATIONS

In June 2017, the world's largest shipping conglomerate was brought to its knees by a massive malware attack that was described as the most devastating cyberattack in history. The screens of all the computers of the huge corporation started turning black in waves, one after the other, irreversibly locked. The entire IT system of the global logistics giant was zeroed in front of the eyes of the helpless SecOps pros. Any mitigation strategy couldn't cope with the fact that the NotPetya strike, which cost A.P. Møller-Maersk between $250 million and $300 million, was entirely automated.

# AUTOMATING SECURITY OPERATIONS: BENEFITS AND ROI

When your data is threatened, speed 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 don't come cheap. When the average large-scale U.S. enterprise deals with nearly 10,000 security alerts per day, it's easy to see how numbers may quickly add up causing costs to hit the fan in no time.

Automation dramatically improves team speed, reducing average time to respond to most threats from 30 mins to 5 mins – that's more than 80% of time saved. 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 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 help 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 duly noted and pasted
- Sending countless notifications to impacted users, often working in different departments or even different cities
- Prioritizing security alerts when the daily volume is unbearably high
- Operational overhead can quickly ramp up to regularly deploy and configure new tools
- Working with complex security stacks can be challenging if all tools cannot communicate with each other

# SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

The Ponemon Institute found that today 75 percent of all organizations in the United States are not prepared to respond to an attack. 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

According to Gartner, the SOAR market is projected to grow from $275 million in 2018 to $550 million by 2023, representing a CAGR of 14.9%. 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 your precious resources. In the current cyberthreat landscape, there's no time to spend your most valuable talent's time on repetitive manual tasks or false positives.

## WHICH TASKS CAN BE SIMPLIFIED BY AUTOMATED SECURITY OPERATIONS?

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

# 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.

Companies with larger security event investigative teams know that an orchestrating tool is just one of the weapons you need to fight the horde of malicious software and malware. 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 required to most efficiently and effectively deal with the mass quantities of raw log data that makes 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 making 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 enriched with threat intelligence, asset lists, geo-location, and other useful information. Once all this data is compiled, the correlation engine would run to create an alert in the system. This is the starting point of the integrations.

The SOAR product will query the alerts on a frequent basis to pull in any new alerts with a specified parameter (name, severity, etc.) and then start kicking off the workflow. When the routine is started, the logging tool can be queried for additional logs which might add a new layer 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 (User Name, 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 on the actual threat. The more they know the better the chance 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 analysts time. The right threat intelligence feed can help you detect all logins from unusual locations or devices, blocking the obvious threat actors attempting to connect with your assets, systems, and network.

However, many stakeholders are concerned that automated threat response may hamper legitimate traffic. The answer is setting a high bar for automated blocking. By aggregating logs, you can set multilayer 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 correlation engine can make more educated alerts, reduce the number of false positives and request an investigation only when a high-priority alert is set.

## INTEGRATING THREAT INTELLIGENCE

Automated security and orchestration solutions are efficient only when they can rely on the correct set of rules. Threat intelligence feeds are required to tell the machine what it is supposed to do with the information it got. The more this information is detailed and reliable, the more efficient the automated response will be. The right 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 in the threat telemetry to the logs that allows for better decision making on the SOAR system as well.

### EXAMPLES OF INTEGRATING LOG MANAGEMENT AND SOAR:

1. Detect a known bad IP addresses via threat intelligence so the IP address is automatically added to the block list on the firewall.
2. Detect 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. Detect a known piece of malware via MD5 Hash and do a quarantine and lockdown event of 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 NotPetya attack taught us a very important lesson — that unless we learn how to integrate automation into our enterprise security solutions, we won't be able to keep up with the evolution of the threat landscape. When a system is able to infect, harvest credentials, move laterally, and then act to wreak havoc to even the most watertight enterprise 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 NotPetya strike happened in 2017. Today, cyber threats are even more sophisticated and dangerous.

www.graylog.org
info@graylog.com

1301 Fannin Street, Suite 2140
Houston, TX 77002