LOGPOINT

The capabilities of SOAR are driving the shift from security analytics to security operations at LogPoint

Nov 02, 2021 10:00 CET

A shift from detection to holistic response

The capabilities of SOAR are driving the shift from security analytics to security operations at LogPoint. In this blogpost, LogPoint CTO Christian Have details the path from detection to holistic response.

By Christian Have, LogPoint CTO

It's not enough to just detect an attack. Adversaries are increasing their speed and sophistication of relentless low-to-mid-level cyber attacks, effectively suffocating organizations by death by a thousand cuts. And how does today's security leadership identify gaps in security to respond to the constant attacks through just detection alone?

CISOs are faced with a barrage of attacks that weaken and challenge the survival of their company. From stealing secrets to impacting operations and holding data ransom with public leaks as the punishment for not paying, CISOs are under constant attack. With cyber attackers continuously trying to weaken defenses over time, it's not enough just to detect incidents. A holistic approach becomes more important than ever.

Shifting from security analytics to security operations

I am beyond proud to say that LogPoint acquired Universal XDR vendor SecBI a couple of months ago. The acquisition was the culmination of an evolution within LogPoint to improve incident investigation that started years ago with our Automatic Investigations (AI) platform.

We designed LogPoint AI to take a data-driven approach to investigations by:

- Analyzing how users of the system acted and repeating the right actions next time an incident popped up
- Analyzing what data was typically associated with an incident and associating similar data next time an incident came up
- Learning from active and closed cases and using the relevant metadata to reapply the learning to other cases

Coincidentally, SecBI researched and built out an Autonomous Investigations capability, which served the same purpose of accelerating triage and investigation.

With the announcement of our new solution LogPoint SOAR, the research and further development of these more advanced features for investigations have found a home.

I'm excited to share our vision for security operations and reflections on how LogPoint's shift from security analytics to security operations will impact our customers in the coming years.

Data-driven decision making for analysts and CISOs

An increasingly critical balance that security teams, particularly security leaders, must strike is on resources spent.

For the CISO, having the ability to determine if a specific security control is valuable and will provide actionable information, all while justifying the cost compared to a different control or an external expert service provider, is invaluable.

The security analyst needs to strike the same balance. Is the analyst working on the right incident, covering the right scope of systems and having the right amount of contextual information about the threat actors' tactics, techniques and procedures (TTPs)?

Monitoring and validating the protection performance of the people, processes, and controls that defend the organization

A curse in security is that you never know when you have done enough. It's not a curse that will be broken any time soon, with changes in threat landscapes, threat actor behavior and advances in detection and response technology. We can't rid ourselves of the curse, so we are forced to evaluate our security posture quantitatively. With the evaluation, we can gain insight into whether our posture is improving or not. Quantitative security posture validation sounds advanced and complex, but in reality, it's pretty straightforward.

Larger organizations know and use breach and attack simulation (BAS) technologies to instrument their security controls and simulate attacker behavior while closely monitoring how the security controls perform. If your organization is ready to work this structured with security posture validation – great! However, to maximize the performance of security teams, procedures and controls, it's necessary to validate against actual attacks.

In LogPoint, we are working with hundreds of organizations to quantify the performance of security controls, not through instrumentation of security controls, but by measuring how well security controls actually perform on a day-to-day basis.

We are revolutionizing how security teams talk about their controls' capabilities and processes with our real-life measurements. We give CISOs a data-driven means to evaluate where to invest in the infrastructure, process landscape or skills domain.

Managing quantitative evaluation of security controls

LogPoint AI measures analyst behavior, playbook performance, orchestration results and can draw up conclusions – let's walk through an example:

Your SIEM generates a Conti ransomware alert

1. An alert was triggered hinting at WMI spookiness (T1047)
    1. Automatically gathers context
2. Connects the alert with the ATT&CK technique
3. Your remediation playbook immediately kicks off
    1. Quarantines the machine
4. Prepares machine for remote wipe
5. Checks the SIEM for similar alerts and logs to contain the breach

Conti has different ways of getting into your network, with the most common by exploiting Microsoft Exchange Server's web platform.

So, what happened? Well, there was malicious activity before our controls were effective. We've learned from evaluating the TTPs of the attacker that Conti behaves by creating a web shell and executing PowerShell scripts to secure more permanent access. Then, Conti launches internal reconnaissance and even moves laterally in the network and so on and so on. SophosLabs has an excellent tools overview that gives us some insight into Conti's behavior.

Notice how late in the chain of events and tools deployed (Lateral Movement) we notice wmic, the kickstart to the SIEM alert.

From a security operations perspective, it's great we detected and possibly managed to prevent the exfiltration and subsequent data encryption – staving off a ransomware attack. However, we detected the attack late, and the cleanup was expensive. What improvements do we have to make as a security organization to move the detection earlier?

- Did we lack adequate endpoint detection and response (EDR) capabilities?
- Did our proxy and firewall capabilities fail us?
- Why was our threat intelligence platform unable to pinpoint Metasploit or mimikatz on the breached machines?

Orchestration is the key to earlier detection

Of course, it's easy to ask questions about what we could have done better. To get ahead of the curve as a security team, we have to instrument our security operations platform. Luckily, the orchestration aspect of security automation is the critical source for improving security operations.

Playbooks will have a hook into EDRs, firewalls and proxies, as well as threat intel platforms.As playbooks mature with the organization and analysts continue to refine them, security operations visibility increases.

If we have a good EDR in place, why isn't it detecting Conti? Did we misconfigure it? Did we assume to have it deployed in all the right places?

Suppose we know a different threat intel vendor claims to have Conti detection. In that case, we know that we could have flagged behavior much sooner and prevented lateral movement with the right TI capability.

When security teams evaluate a new solution, such as EDR, they can put it through its paces with existing playbooks and the existing ecosystem of security controls. The results give us a standard way of evaluating the way we deploy the technology and, of course, the technology itself.

The future of LogPoint SOAR

The capabilities of SOAR are driving the shift from security analytics to security operations at LogPoint. SIEMs that surface an alert are great, but a solution that provides a holistic approach to security operations is preferred. Security operations are more than just the automation of repetitive tasks, orchestrating how security controls perform and playbooks tying everything together. With a holistic approach, you use the data from the execution of playbooks to uncover gaps in controls, processes and even how the security staff performs.

With the gaps identified and a data-driven way to evaluate security performance, CISOs now have a common ground to discuss investments in Product X vs. Product Y vs. MDR vs. Service Z. CISOs can back up their discussions with data that they can present to the security team and the budgeting stakeholders.

Multiplying technology through integration

On the technology side, we are investing in fusing SIEM, SOAR, UEBA and EDR capabilities to support our push toward holistic security operations. Currently, LogPoint SOAR integrates with more than 800 distinct technology platforms and can execute many actions in each product. Integration is the foundation that allows quantitative evaluation but, of course, also enables the automation and orchestration that we design playbooks around.

What's next?

We're deploying LogPoint AI with customers now, and we already see a significant reduction in the time teams spend investigating breaches. Teams can also quantify the way they respond to incidents.

Over the coming months, we will share more about how we will accelerate our holistic approach even further with SaaS initiatives we are working on and additional product announcements. Stay tuned!

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98