LOGPOINT

LogPoint CTO Christian Have predicts that 2022 will be the year if holistic threat detection and incident response.

Jan 14, 2022 10:23 CET

LogPoint 2022 Predictions: The year of holistic threat detection and incident response

By Christian Have, CTO, LogPoint

When the time comes to make predictions for the coming year, we often try to identify that one seismic shift that's going to change everything. Spoiler alert – we see no major disruptors in the cybersecurity market. Instead of upheaval, we anticipate a shift in the way organizations think about their cybersecurity challenges and how they go about overcoming them. This shift represents a more holistic approach to security operations and it has been a

long time coming. Here are a 5 things we can expect:

Accelerated adoption of cybersecurity consolidation and integration platforms.

2022 will witness an accelerated shift away from best-in-class point deployments and toward the adoption of unified and consolidated cybersecurity infrastructures, especially for mid-tier enterprises.

Stepping down from Fortune 500 companies, there are thousands of enterprises in the tier below that lack cybersecurity resources and maturity. They constantly struggle to justify their cybersecurity budget and to see significant improvements in efficiency or reduction of risk as a result of their investments. This cycle recurs because while CISOs may be able to buy best-in-class tools, they often do not have the expertise to leverage a product's highly sophisticated feature set. Beyond that, there is never enough budget or time to integrate the operations of their many tools and ensure that they are getting the expected value from them. For many businesses, best-in-class has not been a winning solution and they will seek a more consolidated and unified approach either from a single vendor – or by leveraging open standards to achieve a unified result.

Cybersecurity automation will take a quantum leap.

AI-driven automation of threat detection and response will allow CISOs to replace human behavior and actions with something far beyond what they ever thought possible. Automation is a journey. Many obstacles must be overcome before a single process can be automated, much less multiple, interrelated processes. Artificial intelligence (AI) and Robotic Process Automation (RPA) technologies have matured to the benefit of many industries – and cybersecurity is no exception.

In fact, AI and automation will prove to be the *only* way to keep pace and counter the ever-changing methods of cyber criminals, their brazenness, and their growing volume of attacks. As we know, a real "quantum leap" is actually quite small, but it has a huge effect. This is the effect that AI-driven automation will have on cybersecurity operations.

Regarding response playbooks: Static OUT. Dynamic IN.

The maturity of AI and automation technologies will drive mid-size enterprises and the MSSPs who serve many of them, to accelerate their plans for SOC automation. With the combination of AI and RPA, we will see the

death of the classic security playbook. The playbooks in use today are static. They require a high degree of sophistication and expertise from the analyst who must consider all attack scenarios (even unknown attacks), how we have responded in the past and how we want to respond in the future. The process is way too time consuming, and it's practically impossible to keep the playbooks current.

With AI-driven or even AI-augmented detection and response, the static playbook will be eclipsed by a dynamic, real-time playbook specific to the incident that is threatening right now.

Based on analysis of incident case data, telemetry readings, historical cases and how they were resolved, threat intelligence from the internet, and other sources, the AI-driven system will create the best playbook on the spot. You can execute the response automatically, or require the analyst to OK the playbook actions. It will be that simple.

SIEM technology in a holistic constellation.

The future of SIEM is important to organizations across the globe. SIEM is here to stay. In the EU, there is regulation driving CISOs to keep their deployed SIEM local either on-prem or with an EU-based cloud provider, and to look for XDR or other consolidation solutions that integrate with it. Here's why. When an enterprise operates in the EU or serves EU citizens, it must verify that every system holding EU citizen personal data has EU-compliant privacy measures in place.

Just recently a new EU regulation came out, stipulating that data about an EU citizen is covered by EU law regardless of where the data resides. This will inhibit enterprises from selecting a cloud-based SIEM that is hosted outside the EU or owned by a non-EU entity. It's almost as complicated to explain as it is to comply with!

Data will drive everything.

Another reason 2022 CISOs will favor consolidation/unification solutions like XDR, is because the unified instrumentation enables a comprehensive data-driven approach to cybersecurity strategy and implementation. When cybersecurity metrics and data are easy to digest and stay above the technical fray, CISOs can engage in performance and funding conversations that are much more productive.

The potential we see for 2022 depends on data. Accurate data. Complete data. Trustworthy data. Real-time data. Historical data. Enterprises need all of it to mount an effective defense against both external and internal threats. They need a platform that pulls all their cybersecurity data together, verifies it, gives it context, simplifies it, and prioritizes it based on urgency, past experience, potential damage, damage already incurred and many other factors. They need data to orchestrate the different tools in their cybersecurity infrastructure, so each tool plays its part fully and to maximum advantage. They need data to automate. If you can't trust your data, you can't automate the processes that use it.

2022 is the year of holistic threat detection and incident response solutions.

The bottom, bottom line? Next year is the year of holistic threat detection and incident response which will rapidly accelerate and be characterized by AI-driven consolidation of capabilities, unified instrumentation and automation. The holistic approach could take the form of an XDR platform, or a home-grown solution. Time will tell.

Lots of cybersecurity companies are investing in the automation side of things. But no matter where you look, vendors are building automation platforms to optimize a 30, 50, or-100-person SOC. These sophisticated and complex platforms have no value for the CISO of a mid-tier business. They are beyond reach in price and practicality.

That is why we see thousands of enterprises moving toward a consolidated and holistic approach that ceases to run after best-in-class tools with lots of bells and whistles, and focuses instead on leveraging AI and automation to make their security operations simple, efficient, and more effective than they ever thought possible.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and BCS technologies converged into a complete platform that efficiently detects threats, minimizes false positives,

autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

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