Alphabet Soup: Making Sense of XDR, EDR, NDR, and SIEM

LogRhythm's Jonathan Zulberg and Andrew Hollister on matching platform to portfolio

LogRhythm™

iSMG
INFORMATION SECURITY
MEDIA GROUP

Contents

Alphabet Soup: Making Sense of XDR, EDR, NDR, and SIEM

Andrew Hollister

As Deputy Chief Information Security Officer, Hollister oversees the LogRhythm Labs team to research threats and deliver world-class security, compliance, intelligence, and operational risk content to protect LogRhythm customers from damaging cyberthreats, help them to meet their compliance needs, and reduce the risk to their organizations.

Jonathan Zulberg

As Vice President of Field Engineering in the UK, Zulberg has worked with and advised a large number of Fortune 500 and government organizations on global security improvement programs for over 12 years. He specializes in information security policy, SIEM, encryption, endpoint security and email security. His current interests in the field include mitigating methods of data exfiltration.

XDR, EDR, NDR, and SIEM. They are among the most prominent acronyms in cybersecurity. But what do they all mean, how do they work, and how do the technologies fit into your security portfolio? **Andrew Hollister** and **Jonathan Zulberg** of LogRhythm share insights and strategies.

In this video interview with Information Security Media Group, Hollister and Zulberg discuss:

- The differences among the platforms
- How you might journey from one to another
- Which product fits best in your security portfolio

EDR, NDR, XDR, and SIEM

FIELD: XDR, EDR, NDR, and SIEM. What do they all mean? How do they work, and how do the technologies fit into one's security portfolio?

ZULBERG: Each one of them is vital and important to an organization, and each one does something unique. EDR stands for endpoint detection and response, and its primary goal is to identify malicious activity occurring at the endpoint. Other technology like network detection and response (NDR), identifies malicious activity traversing hosts; for example, detecting lateral movement across the network.

A security information and event management (SIEM), is a solution that provides an overarching view across the environment. A SIEM consumes the wealth of data from all your assets and security technologies and gives you holistic visibility across the enterprise.

Extended detection and response (XDR) technology is a new player in the market. It combines EDR and NDR functionality with some elements of user and entity behavior analytics (UEBA). People get confused with the difference between XDR and SIEM because they have some overlapping capabilities.

HOLLISTER: SIEM is used for threat detection, compliance, operational risk, and many other things. SIEM collects information from many different sources and as a result, it is a broad and shallow approach. XDR goes narrow and very deep into specific technology areas. It dives into the network to understand the traffic and runs analytics that are specifically attuned to that traffic. It does the same for endpoints as well. EDR, NDR, and XDR are all about detection and response. They're very focused on threat hunting and detection while SIEM can be used for broader purposes.

"XDR will give you a combination of EDR and NDR. It merges these two technologies and looks at what is happening at the endpoint and then laterally. It helps detect when an attack on the endpoint starts to move to the next endpoint across the network."

Jonathan Zulberg

What Are the Benefits?

FIELD: With that context, I want to ask you a series of questions as though I were a security leader looking to find some differentiation here. Let's start with this question: What can these technologies do for one's organization?

ZULBERG: It depends on the technology you procure. For example, from an organizational visibility standpoint, EDR technology provides a great view of threats occurring at the endpoint. It tells you what is attacking your endpoint, host, or server, and the activities being performed by the malicious actor. EDR gives you the ability to respond and mitigate that threat on that endpoint. NDR gives you similar capabilities, but is primarily focused across the network. It tells you what is occurring on your network, who is coming across it, and what anomalies are happening across your network. NDR also gives you the ability to respond to a threat.

XDR gives you a combination of EDR and NDR. It merges these two technologies and looks at what is happening at the endpoint and then laterally. It helps detect when an attack on the endpoint starts to move to the next endpoint across the network. From a visibility standpoint, NDR, UEBA, and XDR give you very deep analytics and security visibility around the threat actor. SIEM will give you that visibility, too. It consumes information from solutions such as NDR, UEBA, and EDR. With SIEM, you invariably get more capability because it's a much broader platform. So you can take all that XDR can do and then use SIEM to layer in additional capabilities, like reporting, compliance, and operational monitoring. It comes down to the requirements of the organization and a team's ability to support the technologies.

HOLLISTER: It also depends on what you already have in your environment, what threats you are concerned about, what threat actors you see against your particular vertical, and what threat access you observe as being operational in your environment. SIEM will give you everything — detection, response, and the compliance piece.

Security leaders need to ask themselves: "What are my priorities? Are there compliance mandates that I must follow? Must I be able to demonstrate compliance with them?" If you need to comply with PCI or ISO 27001 or other such things, then it's likely you'll need SIEM to fulfill those requirements. But if you don't have a specific compliance requirement, you may start your journey with EDR. That will provide protection and visibility on your endpoints, where your users are interacting with devices and resources. Then you can build that up over time toward XDR.

How Do They Differ?

FIELD: What are the differences among these platforms? How would you describe these for a customer?

ZULBERG: EDR is obviously very focused around protecting the endpoint. If a user browses to a malicious website and some sort of malware is downloaded, EDR can stop that threat before it turns into something like a ransomware attack.

NDR analyzes the network. There's always an argument about whether the endpoint or the network is the source of truth. Some people say, "If it didn't hit the network, it didn't happen." We see both sides of that argument; both are true. It's about what's a priority for you in your environment. So NDR is about understanding what's crossing your network. While Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are both good at detecting well-known threats, they are very noisy and the false positive ratio is difficult to handle. NDR adds in analytics and behavioral capabilities that result in high-fidelity alerts.

XDR is the combination of EDR and NDR, providing a compromise on the argument of whether the network or the endpoint is more important. They're both important; they both give a level of visibility into what's happening throughout your environment.

> "EDR is very focused around protecting the endpoint ... NDR analyzes the network ... XDR is the combination of EDR and NDR, providing a compromise on the argument of whether the network or the endpoint is more important."

Jonathan Zulberg

Which One to Start With?

FIELD: Is there a logical journey from one to another?

ZULBERG: Sometimes, but not always. You don't buy one and automatically go on this linear upgrade path to acquiring the other. But in certain organizations, it makes sense to start off on a journey. Where do you place your emphasis and your requirement? Whether you start with EDR, NDR, or XDR comes down to resources available and your ability to implement these technologies and then monitor them for response purposes. If an organization has sufficient resources in place and a broad set of requirements (e.g., compliance and reporting, security, and operational monitoring requirements), it usually starts with XDR. Then as its requirements grow, it upgrades to SIEM. But some organizations start with EDR or NDR and then progress to XDR and later up to SIEM. It depends on the customer.

HOLLISTER: SIEM is all about getting overall visibility across all different types of technologies and across the entire organization, from your firewalls through your network infrastructure and perhaps to web applications and other types of SaaS products as well. The strength of SIEM is its very broad visibility.

ZULBERG: It's important to understand that you can use SIEM for additional visibility. Organizations use it to identify and monitor breakages in business processes. Those are not necessarily security or operational threats. They're simply business process breakdowns, which can be identified and then rectified. The power of the SIEM is that it can see everything. EDR, NDR, and XDR can see a lot, but only in a very small window of information.

HOLLISTER: There's a lot of talk in the industry about whether XDR is the "easy button." To some extent, it is, because it's much more focused. You can look at networks and endpoints. That's a very slimmed-down view of what SIEM tries to look at. SIEM looks at many different technologies and there are a variety of different things that you can do. It's a very mature space containing significant platform-based offerings—and that brings with it a level of complexity. If you don't have all the requirements to drive the need to acquire SIEM, the overhead can be more than you are either prepared for or able to support. In that scenario, XDR may be a good step for you.

ZULBERG: It's like comparing a speedboat to a warship. Both go in the water and do similar things, but one takes a lot more feeding and watering and provides a lot more protection. One's very easy to drive, but you can't do as much with it. So you get there quicker, but you won't be able to see as much.

How to Choose?

FIELD: How would you counsel a customer about which of these products best suits the security portfolio they are trying to build?

ZULBERG: You have to understand the customer's requirements, infrastructure, and technology already in place. If a customer has UEBA, EDR, and NDR, purchasing an additional XDR is not going to be a great alternative for them because they're going to get so many overlapping functionalities. In that scenario, a SIEM may be a better solution to amalgamate and merge that information together and get that visibility we described. But it's also about the resources available to drive this technology. None of these technologies we're describing are installed and left to their own devices. Each one will require feeding and watering, and you need to understand the information it presents to you. So it comes down to the skill sets of the individuals within the organization and the size of the organization. There's no one answer for any of this. You have to apply the right technology to the right circumstances.

HOLLISTER: We look at the problems the customer has and the issues they are concerned with and then align the technology solution to those problems. A lot of technology challenges can be solved through SIEM, while XDR, EDR, and NDR are much more focused on specific areas.

> "We look at the problems the customer has and the issues they are concerned with and then align the technology solution to those problems. A lot of technology challenges can be solved through SIEM, while XDR, EDR, and NDR are much more focused on specific areas."

Andrew Hollister

The LogRhythm Approach

FIELD: How is LogRhythm helping its customers to navigate this alphabet soup we've just talked about?

ZULBERG: We sit down with our customers and our prospects and help them understand the value of each one of these technologies, what the technology brings to the organization, and how they can take advantage of it and use it. We have a conversation to arrive at a logical conclusion that is the right fit for the organization, based on many factors.

HOLLISTER: We take a consultative approach. We try to understand what the customer has in place already in terms of the technology that they're using, the business outcomes they're trying to achieve, and what's most important to them to protect. We look at the problems they need to solve at this point in the maturity of their organization and their cybersecurity capabilities. We look at what tooling actually fits into where they are in their cybersecurity journey.

ZULBERG: We try to drive our customers away from buzzwords and help them understand what benefit these technologies will bring them. Sometimes a technology will not benefit you, and there's no point in trying it. It will just add to your overhead in terms of the operational management. We become a trusted adviser to our customers, and articulate the value that each one of these solutions brings. We unravel the needs of our customers, and then align the correct solution to mitigate their problems.

> **"We try to understand what the customer has in place already in terms of the technology that they're using, the business outcomes they're trying to achieve, and what's most important for them to protect. "**

Andrew Hollister

About LogRhythm

LogRhythm helps busy and lean security operations teams save the day — day after day. There's a lot riding on the shoulders of security professionals — the reputation and success of their company, the safety of citizens and organizations across the globe, the security of critical resources — the weight of protecting the world.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an ever-changing threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.

The LogRhythm SIEM Platform helps organizations around the globe reduce cyber and operational risk by rapidly detecting, responding to, and neutralizing damaging cyberthreats.

Together, we are ready to defend.
Learn more at logrhythm.com.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY®
CU INFO SECURITY® Just for Credit Unions
GOV INFO SECURITY®
HEALTHCARE INFO SECURITY®
infoRisk® TODAY
CAREERS INFO SECURITY®
~~Data Breach~~. Prevention. Response. Notification. TODAY
CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io

www.logrhythm.com // info@logrhythm.com

United States: 1.866.384.0713 // United Kingdom: +44 (0)1628 918 330
Singapore: +65 6222 8110 // Australia: +61 2 8019 7185