MDR and SOC and MSSP and SIEM and EDR and XDR and SOAR, Oh My!

A Security Operations Guide

NEXUM, INC.

Ron Temske, Vice President of Strategy
Chris Currin, Director of *first*defense* MSSP Sales

Contents

Introduction

In the world of cybersecurity, there is no shortage of terminology to describe the technologies that keep an organization safe. Specifically, the abundance of technical language is overwhelming when it comes to the security operations that detect and respond to threats. What's worse is that these terms are used interchangeably and sometimes inaccurately.

A few examples are:

- Managed Detection & Response (MDR)
- Security Operations Center (SOC)
- Managed Security Services Provider (MSSP)
- Security Incident & Event Management (SIEM)
- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Security Orchestration Automation and Response (SOAR)

Knowing the differences between these concepts and how they work together is critical. To stay ahead in today's environment while also positioning your organization for the future, you need to look beyond buzzwords and understand the desired outcomes of your security strategy. And the best security strategy uses each of these services to complement each other.

This guide will examine these terms, their meaning, and how they relate to each other. We'll also provide our thoughts to help you fully leverage these technologies.

The Future of Cybersecurity is Evolving

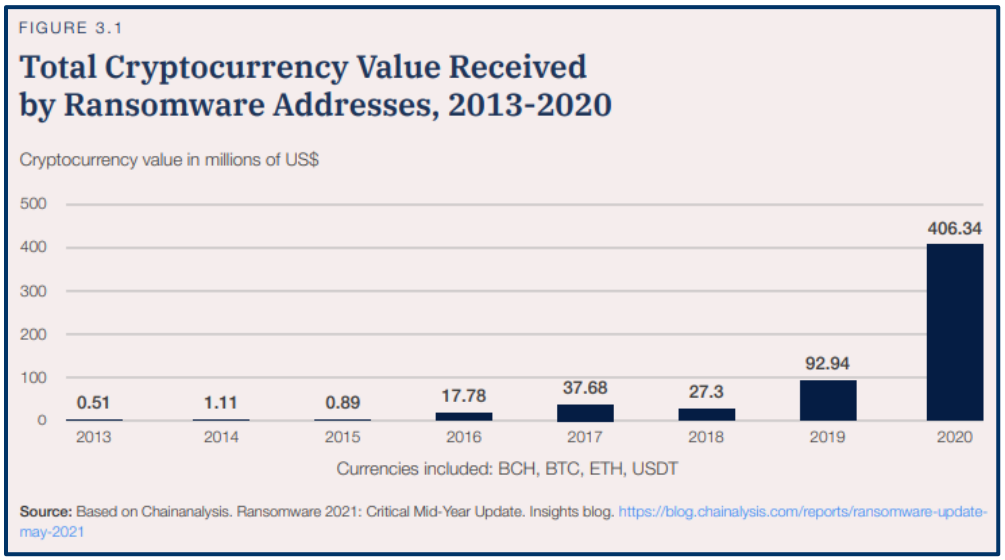
Ransomware and cybersecurity attacks constantly threaten every business, no matter what industry you're in. The key to success is earning and keeping customer trust. Consumers today are well-informed about cybersecurity threats and expect your organization to prioritize data protection. However, staying ahead of threats in 2023 and beyond will only get more challenging and expensive.

Warnings from the FBI, compliance requirements, federal guidance, and general "sleep well at night" concerns have every business working to improve cybersecurity. The threat landscape constantly evolves, creating a more complex environment every day.

According to the World Economic Forum Global Risk Report 2022:

- There was a 435% increase in ransomware globally in 2020
- There are three million unfilled vacancies worldwide for cybersecurity professionals
- Digital commerce is expected to grow in value by USD 800 billion by 2024
- 95% of cybersecurity issues are traced to human error

"Malicious activity is proliferating, partly because of the growing vulnerabilities—but also because there are few barriers to entry for participants in the ransomware industry and little risk of extradition, prosecution or sanction. Malware increased by 358% in 2020, while ransomware increased by 435%, with a four-fold rise in the total cryptocurrency value received by ransomware addresses. 'Ransomware as a service' allows even non-technical criminals to execute attacks, a trend that might intensify with the advent of artificial intelligence (AI)-powered malware."



Cybersecurity and ransomware risks have the attention of small businesses, enterprises, and governments. Recognizing these challenges is the first step to addressing the problem and protecting your organization. How we manage the risks and work to mitigate and defend against cyberattacks becomes the everyday work effort for the average security team.

Security Operations Terms

Let's look at these terms and how they work together and relate to one another.

Managed Detection and Response (MDR)

MDR is a security service providing access to the tools and security expertise an organization needs to protect itself against cyber threats. An MDR provider offers round-the-clock security monitoring, incident investigation, and response with deeper visibility and more granular protection.

A good MDR solution is designed for advanced technologies that extend to the endpoints, cloud, and software as a service (SaaS) environments. It incorporates specialized expertise, such as threat hunting or cloud security. These solutions perform the complex tasks of triaging advanced threats, performing forensic analysis, and identifying compromised networks and systems. The MDR service will also provide recommendations on an appropriate response to the threat or issue detected. These might be applying patches, making rule changes in a firewall, quarantining an infected system, and other measures.

MDR services frequently leverage the capabilities of multiple sources of threat intelligence. Put simply, threat intelligence is the documentation of suspicious behaviors or sites shared across various organizations. This could be as simple as a range of IP addresses aligned with a suspected threat actor or more specific information such as attack techniques. By leveraging threat intelligence, an MDR service is better equipped to rapidly detect the newest threats.

Security Operations Center (SOC)

This term can be confusing because it can be used to describe a place or to describe a set of services. In the literal context, a SOC is a place or group of people focused on an organization's security operations (or as a service provided to other organizations). When describing services, SOC frequently covers a wide range of offerings that an actual SOC would deliver; essentially, many of the terms we're defining in this guide are services or functions that a SOC would provide. "SOC as a service" is also a term that's used, and generally refers to purchasing these services from an outside entity.

Managed Security Services Provider (MSSP)

While sometimes used interchangeably with MDR, an MSSP typically focuses on security architecture and devices. MDR is more focused on the data coming from those devices. When the two services are combined it can be quite effective, as the devices' security alerts, configuration, and upkeep are maintained in harmony. It's worth noting that an organization may offer MSSP services, MDR services, or both.

Security Incident and Event Management (SIEM)

SIEM is another term that's used in multiple contexts. While sometimes used to describe a service, SIEM is technically a software tool. SIEM is used to collect and collate logs from various security information sources. SIEM can also apply rules and correlations to help identify potential threats of suspicious behavior. For example, a SIEM rule might create an alert if the same account were authenticated from multiple geographic locations in a short period of time (the impossible travel rule). Generally speaking, SIEM solutions cannot implement any changes or provide protection directly, but can be a beneficial source of information to guide remediation activities.

Many compliance and regulatory measures require the retention of security logs for some time, and SIEM is typically the tool used to provide that log collection and retention.

Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)

Welcome to the most confusing, abused term in security today: XDR. Here is a little history to understand the evolution of these terms. The initial endpoint platforms we used for years, sometimes called antivirus or anti-malware, became known as endpoint protection platforms (EPP). These systems were based primarily on signatures that had to be updated regularly and typically couldn't detect or protect against any threat if there wasn't a corresponding signature.

The next evolution was EDR. The basic idea of EDR vs. EPP was that EDR added machine learning and behavioral analytics to detect previously unknown threats, even if no signature was in place. While EDR promised to end malware and catch all threats at the endpoint, the reality is that the cat-and-mouse game persists as threat actors continue to find ways to bypass detection. EDR could alert on suspicious behaviors without requiring an underlying signature. For example, attempting to overwrite a system file would be considered suspicious behavior; EDR could either deny the action or prompt the user to verify the action was intended.

XDR combines the concepts of EDR and SIEM to provide a more holistic solution that adds the capability of direct response actions. Where SIEM focuses on log collection and data analysis, XDR offers greater insight into threats and adds the ability to automate response actions directly. When a threat is detected, the capability exists to make rule changes or quarantine devices automatically.

Security Orchestration Automation and Response (SOAR)

SOAR is the last of our terms, but not the least confusing. As the name implies, SOAR primarily automates and orchestrates response action in your security environment. As a side note, XDR is frequently advertised as providing most of the benefits of a complete SOAR platform without all the cost and complexity.

Proper implementation of SOAR can provide tremendous benefits for an organization, but adequately tuning the automation can be time-consuming and difficult. Few things are more frustrating than launching a denial-of-service attack against yourself due to an overly aggressive SOAR platform! When implemented correctly, however, a SOAR solution can automate many tasks and reduce the labor required. Given the challenges in recruiting covered above, this can be pretty valuable.

As you can see, there is much overlap between these terms, and it's no wonder many people find them confusing. Let's not allow ourselves to get overwhelmed by all the acronyms. Instead, we can focus on the core capabilities required. These concepts can be compelling when integrated into a holistic security detection and response solution.

Where to Begin

Assessing risks and managing vulnerabilities will help reduce your attack surface. But no cybersecurity solution will ever eliminate the possibility of threats entering your environment. That is why rapidly containing a threat is critical. The longer it takes you to mitigate, the higher the likelihood that a security incident turns into a full-blown data breach.

Knowing the common vulnerabilities is a start, but you must also know how to defend against them. Here are a few critical pieces of advice to get you started:

1. The most crucial function many of these services provide is visibility. Properly securing your environment is virtually impossible if you lack visibility into events and traffic. With the concept of visibility comes the need to gain that insight into all areas of the organization. When moving to the cloud, it can be challenging to gain visibility with both Infrastructure as a Service (IaaS) and complete SaaS solutions, but it is still possible.

   As a side note, all the major cloud providers publish a guide outlining the roles and responsibilities for security between the provider and the customer. Many organizations don't take the time to understand this division of responsibility fully. They are unpleasantly surprised when an incident occurs and realize the cloud provider has no responsibility to protect against that situation. We strongly recommend reviewing the responsibility matrix for all your cloud solutions and ensuring that your organization understands where the cloud provider's responsibility ends and yours begins.

2. Concerning visibility, we frequently see two things that could be improved at opposite ends of the spectrum. The first is limiting the number of monitored data sources (usually due to the cost of storing logs or bandwidth concerns of sending too much data). This mistake can result in missing key events and not catching a potential security issue as quickly. The second mistake is feeding enormous amounts of data into the system but not taking the time to tune out the noise properly. In this case, all the necessary alerts are coming through, but the noise of all the false positives can mean that the tools are largely ignored. In both cases, critical events can go unnoticed.

3. Another issue is the tendency to focus on niche solutions while not correctly handling the fundamentals. We see organizations spending money on security solutions that demo well (and are great solutions) but only address a niche problem while not properly shoring up the fundamentals. When building a house, worrying about a seam in your sheetrock while ignoring that the foundation is sinking is putting your attention in the wrong direction!

The Decision to Partner

Whether to bring in outside help for security or handle everything in-house is a difficult decision. The reality is that you can combine the best of both, leveraging partners where it makes sense while keeping some functions in-house.

Your team will understand your unique business requirements more thoroughly and are necessary for an effective security strategy. A partner can provide added value through the expertise gained from delivering security solutions to hundreds or thousands of customers. They will have greater visibility into macro trends and issues facing the security community. A partner may also be better able to tune out false positives and respond more quickly in an event with root-cause analysis and compensating controls to address the situation.

The key is finding a partner with the right mix of technology expertise, customer service, and the ability to customize their services to meet your needs.