Brought to you by

CISCO

Extended Detection and Response (XDR)

for dummies®
A Wiley Brand

2nd Cisco Special Edition

Explore the value of an XDR platform

Experience better threat detection

Reduce complexity for your security team

James Sullivan
Dan Sullivan

About Cisco Secure

As the largest enterprise cybersecurity company in the world, we lead the way with cloud-native and cloud-delivered solutions that secure everything and everyone your network touches. Cisco Security Suites help you detect and respond to the most sophisticated threats and ransomware with correlated cross-domain telemetry and AI/ML driven enrichment to increase security efficacy, improve experiences, and optimize economics.

cisco.com/go/security-cloud

Cisco XDR is an extended detection and response solution that integrates with the broad Cisco security portfolio including endpoint, network, cloud, and email as well as many third-party offerings. This ensures organizations can gain a unified view across the security stack to enable faster, more simplified investigations, to reduce false positives, and to enhance threat detection and response through clear prioritization of alerts, providing the shortest path from detection to response.

cisco.com/go/xdr

Extended Detection and Response (XDR)

2nd Cisco Special Edition

by James Sullivan and Dan Sullivan

for dummies®
A Wiley Brand

Extended Detection and Response (XDR) For Dummies®, 2nd Cisco Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-26618-0 (pbk); ISBN 978-1-394-26619-7 (ebk)

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Jennifer Bingham

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Account Manager: Jeremith Coward

Content Refinement Specialist: Tamilmani Varadharaj

Table of Contents

Introduction

IT security is one of the fastest changing realms of the tech world. There are new tools, techniques, and kinds of attacks popping up all the time. One of these new tools is extended detection and response (XDR). XDR platforms include tools for orchestration, monitoring and analytics, automation, visualization, and more. What brings it all together is a centralized viewpoint of your entire security infrastructure.

Enterprise security environments have gotten so complex that siloed security resources are no longer a viable option. Attackers are exploiting multiple attack points, regular business activity is too easily misidentified as malicious, and security teams are already up to their ears in legitimate threats.

Security information and event management (SIEM) and security orchestration automation and response (SOAR) solutions share some features with XDR, but there are some key differences. SIEM often can't properly organize and process all the logs and alerts it generates. SOAR, on the other hand, doesn't have the integration capabilities that XDR does. However, these two tools still have their places in the security landscape.

This book discusses what exactly XDR is, how it relates to other security solutions, how it can integrate with those solutions, and what challenges XDR is attempting to solve.

About This Book

XDR is a new addition to the IT security world, so not many people have a full grasp of it yet. That's why this book exists! *For Dummies* guides are easy to read and the information is easy to digest, but they also provide the reader with the information they need to make decisions, get things working, or just learn something new.

Maybe you want to learn about a specific part of XDR. No problem! Even though each chapter has something to add about XDR or IT security in general, feel free to skip around. Each section in this book stands on its own and can be approached without reading everything that came before it.

If you really want a condensed version of this book, check out Chapter 6. There you'll find ten of the most important points about XDR from the rest of the book. It's a great way to get a jump start on the book's contents, or just speed into knowing stuff about XDR!

Icons Used in This Book

While reading you might come across a couple of special symbols. We use these to point out special information or provide reminders for important points from the chapter. Here are the icons you'll find in this book:

REMEMBER

This icon is used to highlight a critical point from the chapter. It might be something specific about a security tool or a general concept. This information probably shows up more than once.

TIP

This icon is meant to add a little something extra to a section. It might elaborate on a point or add something that didn't fit into the main section. Tips are usually specific and not about general concepts.

Beyond the Book

If you still have questions or want to learn more about XDR and IT security, head over to `cisco.com/go/xdr` or `blogs.cisco.com/security` to read about what the folks at Cisco think about the state of IT security.

IN THIS CHAPTER

- » **Evolving security threats**
- » **Looking at modern security tools and techniques**
- » **Breaking down XDR**
- » **How Cisco does it**

Chapter 1 Security Operations: Trends and Challenges

The cybersecurity landscape today is daunting. New threats and threat actors emerge on a seemingly daily basis, including from nation states, cyberespionage, misconfigurations, vulnerabilities, and more. Plus, a vast number of vendors and tools are in the market today, which can sometimes create chaos when trying to get the products to "play nicely together."

This chapter looks at some of the most prominent security tools available today, how they're different from each other, and what the new kid on the block, extended detection and response (XDR), brings to the table. But first, some info about how security threats have evolved in recent years.

The Evolving Threat Landscape

When it comes to cyberattacks, ransomware, vulnerability points, malware, and more are all on the menu. The number of security threats is growing just as fast as their complexity.

Here are a few of the biggest threats:

- **Ransomware:** Yes, this is still around. Ransomware is an attack that locks target data to hold it hostage. The recent Colonial Pipeline attack is a high-profile example of how powerful this threat can be.
- **Phishing:** The goal of phishing is to trick victims into sharing sensitive information or install malware by convincing them the message is from a trusted source. Phishing has evolved into a variety of forms, including *spear phishing,* which targets a specific person and *smishing,* which uses SMS messages rather than email.
- **Living off the land (LOTL):** LOLT attacks use tools and system components already installed on a system. This has a significant advantage of allowing attacks to blend in and help avoid detection. LOLT attacks also enable attackers to maintain long-term presence on a network while they steal data or set the stage for the next phase of an attack.
- **Nation state and government level attacks:** These are any cyberattacks originating from state actors. With the attacks on Sony and the U.S. Treasury Department, state-sponsored attacks continue to be a relevant threat.
- **Malware and other viruses:** Yet another tried-and-true attack strategy, malware is any software made to disrupt or damage internal systems. These threats continue to increase in complexity but can often come through simple delivery methods. For instance, “urgent” emails advertising false Windows OS updates are on the rise.
- **Insider attacks:** These are attacks carried out by members of your own organization. While this type of threat isn’t often talked about, it’s just as important. Even after pre-employment screening, a bad actor may slip through the cracks into an organization. A common insider attack is proprietary information leaks and trading.

It’s easy to become overwhelmed by cybersecurity concerns, and yet this is the cost of doing business digitally. In the end, security is about maintaining control of your resources and infrastructure. Outside parties will often try to penetrate your network, steal or destroy your data, and maybe even compromise hardware. These are risks you have to take, and prepare for, while reaping the benefits of working in the digital space.

Security Tools and Techniques

Like the security threats organizations are facing, the security techniques and security are also evolving. We have moved past "a firewall and a prayer" being enough to secure customer data and network integrity. (Not that this means you don't need a firewall — you still need one.)

In true tech-sector fashion, there are buzzwords, abbreviations, and acronyms flying in every direction in the security solution space. This book takes a look at three types of security solutions employed to improve automation and threat detection: security information and event management (SIEM), security orchestration automation and response (SOAR), and extended detection and response (XDR). First, let's talk about the silo problem.

Siloed solutions and their limitations

The common practice of siloing distinct portions of a digital infrastructure has many benefits. It keeps things organized, allows developers and administrators to focus in on the information relevant to them, and is often how solutions and tools are meant to be used. However, problems arise when disparate systems have information relevant to the function of other siloed systems.

This problem is especially noticeable when dealing with security solutions. Endpoint security collects and processes different kinds of information than network security or email security. All of these systems, though, benefit greatly from a holistic view.

REMEMBER

Recently there have been innovations and solutions for bypassing the limitations of siloing security solutions. The two most prominent solution types from the last five years are SIEM and SOAR.

Early attempts at integration: SIEM

Security information and event management (SIEM) is a fairly successful, well-tested take on log-and-event management solutions. At its core, SIEM is about gathering as much log information as possible from all over an organization.

Many SIEM solutions can take log data from Internet of Things (IoT) security tools, firewall event logs, and everything in between. This kind of solution starts to break down the silo walls, integrating with multiple solutions and centralizing important security information.

What SIEM doesn't do is give security engineers a boost in threat response time and efficacy. Seeing the security landscape of your organization is great for many things but responding to threats is just as important.

Early attempts at threat response: SOAR

Security orchestration automation and response (SOAR) takes a lot of what makes SIEM great and adds extra layers to account for some of the older solution's weaknesses. Like SIEM, SOAR solutions take data from different parts of the security infrastructure and put it in one place — which is the "orchestration" part.

Automations enter the picture with the ability to put this collected information to use. Many SOAR solutions offer options to automate various auditing, log, and scanning tasks. Automation can't take care of everything, however, and sometimes a human needs to step in.

The "response" part of SOAR is about organizing and managing the response to a security threat. This feature set utilizes orchestration and automation information to help security staff make decisions and respond to threats.

REMEMBER

SOAR automation doesn't automate responses to security breaches. It automates simple analysis tasks to reduce security personnel workloads.

What Is XDR?

Extended detection and response (XDR) is a recent addition to the swarm of acronyms bouncing around the business technology space. It takes a lot of what makes SIEM and SOAR useful and tries to add a little more to each function of the more established solution types.

The basics of XDR

While SIEM and SOAR emphasize logs and analysis — what ends up in the hands of security staff — XDR solutions focus on the endpoints themselves. This is where the action is. This is what the outside parties are attacking.

In this way, XDR shares a lot with EDR (endpoint detection and response) — notice that this is why XDR couldn't be called EDR. What XDR does is *extend* the capabilities of a traditional EDR solution, in addition to deepening the functions of a SIEM or SOAR solution. For example, XDR extends the visibility and detections available with an EDR solution with data and detections from the Network Detection and Response (NDR) solution.

The methodology here is that the time between logging suspicious behavior and recognizing it as an attack, forming a response plan, and carrying out the plan should be as small as possible. To better understand XDR solutions, it's good to break down what they're made of.

Components of an XDR solution

XDR is a newcomer to the security space and there is still some variation in what these solutions offer. However, there are a few key functions XDR solutions provide:

- **Flexible integration:** The amount and method of integration with existing security solutions depends on the XDR solution itself, but there is often a way to incorporate security tools, especially endpoint security, into an XDR platform.
- **Centralized view:** XDR wouldn't be much without a central view of the information it's collecting. XDR looks at most, if not all, of your security environment, and you need a central hub to parse all that information.
- **Artificial intelligence:** XDR platforms incorporate AI to address the increasing difficulty of detecting threats in rapidly growing streams of ingested data. This is especially helpful in lowering response times because security personnel have less work to do before they get to solve a security issue.
- **Automation:** Like SOAR solutions, XDR uses automation to reduce SecOps workloads. It only automates simple tasks, but every little bit helps.

Depending on the vendor, there may be extra bells and whistles attached to an XDR platform, but these should be the foundation of every XDR solution.

Why Does XDR Matter?

SIEM, SOAR, NDR, and EDR are all useful in their own ways. XDR is a new addition to the security solution market, so it needs to bring something that can't be found anywhere else. The real benefit of this new option is not just the new features it brings, but also how these features are responses to the current security landscape.

New security challenges

Cyberattacks are becoming more sophisticated, and not just in how they're perpetrated. The "where" is also changing. With IoT and the continued expansion into the cloud, networks are more numerous, endpoints are growing rapidly, and nefarious outside parties know it.

Now, attacks can arrive at multiple networks and endpoints at once. There are multipronged attacks happening that need new kinds of IT security. SIEM and SOAR solutions simply aren't built to process and manage these kinds of attacks. EDR and NDR are more able to handle them but don't have the management support required to quickly respond to sophisticated threats.

Diverse information sources

Not only are the kinds of attacks becoming more sophisticated, so too are the IT environments in which organizations are working. New potential attack sites are added every day. IoT, cloud applications, and database use are growing quickly. The push to work from home is especially of concern now. This style of doing business is spreading out and increasing the number of devices that have access to internal resources.

Here are some of the challenges brought by working from home:

- The number of devices that need protecting has increased, meaning more points of attacks for outside parties to exploit.
- The variety of employee devices has increased. Many organizations no longer rely only on "work computers." This can require an equally diverse set of security solutions.

- Home networks are rarely as secure as in-office networks. Most employees in an organization are not security experts and cannot guarantee a consistently secure network connection.

This all adds up to a complex ecosystem that requires a complex suite of security solutions. The desire to silo these security tools and information sources is obvious in this light. XDR matters because it lets organizations carry disparate security tools in their security environment while not bringing security operations to a crawl.

Overburdened security staff

IT security professionals are highly skilled and knowledgeable, but there is a limit to what any person is capable of. The complexity and breadth of modern security ecosystems often leads to security engineers getting overworked which, in turn, leads to security operations mistakes.

SIEM and SOAR solutions, while useful in the right context, often leads to an information overload due to their "collect everything" nature. SIEM is notorious for becoming just a new way to dump logs into a pile without any tools to deal with them. The amount and diversity of information being generated by security tools is just too much for a human to handle without machine aid.

TIP

It might seem like I'm being overly negative towards SIEMs; however, it is worth noting that these solutions are very useful for compliance-heavy industries where piles of logs are exactly what you need!

Overburdened, overworked security staff are a recipe for two things: security breaches and unhappy employees. It is truly a lose-lose situation. The way XDR focuses on the endpoint security and task automation means a reduced workload for security professionals.

Primary goal: Reduce MTTD and MTTR

Reducing the mean time to detect (MTTD) and mean time to respond (MTTR) are the end goals of any security operations team. Really, they're the reason IT security teams exist in the first place.

MTTD and MTTR are what they say on the box: How long does it usually take to find and deal with a security issue? Needing to sift through alerts and logs to find real security concerns increases time to detect, while a lack of automation and analysis tools increases time to respond.

XDR is the most recent entry to the security landscape that attempts to decrease both MTTR and MTTD. Collection, analysis, automation, and centralization (all key facets of XDR) aid in speeding up detection and response times. At the end of the day, isn't that exactly what a security solution should do?

Cisco Secure's Approach

Cisco Secure's XDR approach is built on an integrated platform experience. XDR is about organization and control, so Cisco Secure has broken down what it sees as the key components of any successful extended detection and response solution:

- **X:** The platform should cover as many control points and data sources as possible. A security solution is only as good as the vulnerabilities it can cover.
- **D:** Artificial intelligence-supported analysis is increasingly important for detection and decreasing MTTD.
- **R:** Automation and centralized security information means faster response times and streamlined security breach investigations.

Another key part of Cisco Secure's philosophy is that each of these promises from XDR is equally important. The reach of an XDR platform doesn't mean much if it doesn't have automation to support routine security analysis tasks. Lastly, Cisco Secure tries to make integration with security products already in your environment as easy as possible. XDR isn't trying to replace these security tools but strengthen them by breaking down silo walls and streamlining security operations.

IN THIS CHAPTER

- How siloed solutions create roadblocks
- Unsolved problems for enterprise security operations

Chapter 2 The State of Detection and Response

The current landscape of threat detection and response shares a lot with other IT sectors. There are more tools than any one person could keep track of, vendors have different names for the same concepts, and the complexity of IT environments is so great that siloing has become common practice.

Despite the myriad tools available to security professionals, there are still unsolved problems facing SecOps teams. Keeping a low mean time to detect (MTTD) and mean time to respond (MTTR) is a constant struggle, and false positives bog down teams with unnecessary work.

Before looking into the unsolved problems, first take a look at some ways that siloing is slowing down security teams.

Siloed Solution Roadblocks

Placing solutions in silos was a response to the intricate, vast web of ecosystems and security tools that protect them. The idea was that separating different areas of security into their own environments would reduce complexity and make them more manageable.

Instead, these silos highlight the challenges of managing and protecting a modern enterprise ecosystem. They're complex for a reason. Networks, applications, and databases are all part of a greater whole, not freewheeling loners that can wander the wilderness, living off the land as they go.

Each of these siloed sections faces their own challenges from being siloed. Take a look at some examples.

Network security

Network security is the padlock on the door to all of your cool stuff. It includes:

- Firewalls
- Intrusion prevention
- Network access controls

This isn't an exhaustive list of network security functions, but it includes a few of the most important tools. The network security silo includes information on IP addresses attempting to join the network, network traffic volume, port integrity, and more.

REMEMBER

What network security can see reveals what it can't see. Attackers can employ long-running campaigns that use natively available tools making detection difficult. After gaining access, attackers can make lateral movements to probe for other vulnerabilities. XDR can analyze extended data sets that span long periods of time across a wide range of network components.

Application security

Application security involves protecting applications and their resources, which includes servers, databases, messaging systems, and other software infrastructure. This security silo covers a lot of ground, between database authorizations, CPU usage monitoring, input/output monitoring, and more.

Similar to how network security can be slowed down and disrupted by not having all the information on unusual behavior, application security needs to see more than just its own environment.

Take an I/O spike as an example. Say an extreme change in network demand occurs in the middle of the night. It's not during regular working hours, lots of data is moving in and out through an application, and application security is alerted. This could signal some sort of data breach, or it could be a test run of a data migration process by a separate department.

What if there is a big jump in CPU usage that seems unusual? That could mean there is malicious software running on a virtual machine or exploiting an application vulnerability. Or it could be something harmless and part of regular business operations.

In both cases, the silo is creating extra hoops for security teams to jump through, instead of allowing them to move efficiently by not wasting time checking and rechecking that all the activity is aboveboard.

Endpoint security

Endpoint security also covers a range of security tools. Anti-malware, data loss prevention, and endpoint device threat detection all fall under the endpoint security umbrella. The volume of endpoint security tools is increasing, adding to the complexity of this area, with the push to work from home. More devices need access to internal resources, meaning more security is needed for more devices than ever.

Endpoint security itself doesn't get as many security hiccups from the security silo as other security areas, but it does cause issues for other teams — such issues as identity management and network security.

Identity and access management

This one is a bit of curveball. It doesn't even have "security" in the name! One of identity and access management's (IAM) big jobs is managing authentication. This is an umbrella term that covers:

- Two-factor authentication
- Digital certificates
- Usernames
- Passwords

Depending on what's being accessed, industry regulations, and organization-specific policies, one or more of these points will determine the specific login authentication needs.

A simple example of silos throwing a wrench in the gears here is failed login attempts. Repeated login failures, whether it's a misremembered password or username, or something else entirely, can look like an attempted attack to both application and network security teams.

Since IAM covers service account identities, it crosses over with application security in resource-use authorization. To decrease MTTD and MTTR, it is especially important to un-silo network security and IAM.

Unsolved Problems Challenging Enterprises

The business technology sphere evolves at breakneck speed, but there are still plenty of problems causing headaches to developers, admins, security professionals, and business leaders. MTTD, MTTR, cyberattack false positives, and incident triage inefficiency are all issues still facing enterprises.

MTTD

Mean time to detect (MTTD) is a critical part of enterprise security. MTTD is the amount of time it usually takes for a security team to find and confirm that a security breach has happened. Getting to a low MTTD is more than just picking up an alert and finding the attack site.

Detecting a threat or ongoing attack involves looking at multiple interlocking systems and coordinating communication between teams in charge of those systems. For instance, if a network administrator notices activity that looks like a database infiltration, the activity needs to be cross-referenced with the database teams to see if the activity is actually supposed to be happening.

The challenge here is coordinating detection quickly, while not losing accuracy. Speeding past confirming the validity of a threat leads to even more wasted time and resources.

MTTR

The clock on the mean time to recovery (MTTR) starts ticking right after a security problem has been identified and confirmed. MTTR is the average measure of how long it takes security teams to stop or fix the problem. The big questions for MTTR: What has been compromised and how do you fix it?

The biggest challenge in responding to a threat is often that the scope of the IT environment is so large that it's difficult to see all the damage that was done. This is difficult for several reasons and depends on the context:

- IP addresses may need to be found and checked with network security in the case of a network-based attack, but if the breach already happened, where else did the attacker go?
- If a database was breached, it can be difficult to see exactly which tables were accessed, whether the information the attacker gained allowed them to access other parts of the system, and so on.
- The attack may be multipronged with the attacker breaching several points of entry.

Each of these problems requires a different solution, and this solution has to be tailored to the specific situation. Do you have to push a quick software update or fix a vulnerable library? Do you have to block an IP address port to prevent further attacks? The answer might be a mix of things and deciding on the right response recipe is just as important as finding the breach in the first place.

False positives

In the context of security, false positives are benign activities that are misidentified as security threats. A database admin may have just gone on her lunch break after starting a big export job. Meanwhile, a network security employee cancels his lunch because he sees a large volume of network traffic he wasn't expecting. To make matters worse, his lunch was supposed to be a delicious looking chicken katsu sandwich. What a terrible waste!

False positive security breaches not only cause unnecessary disruptions and wasted time, but they also inadvertently let real security breaches slip through. Alert fatigue is like the boy who cried wolf. Say that, on average, an application security team gets ten security alerts every day, but only two of them are legitimate threats. A few days of this isn't a problem, but weeks of false alerts leads to the team not paying much attention to alerts. After all, chances are it isn't a real threat.

False positives, then, are an especially big challenge for security teams. Not only do they waste the valuable time of security professionals, but they can also lead to more security threats getting through your line of defense.

Incident triage

Incident triage shares a lot of the same issues with MTTR. While MTTR is concerned with the time it takes to resolve an issue, incident triage is about prioritizing steps to recover from the incident.

Like all other challenge spots in this section, context is the key here. There has to be an understanding of the impact of the security solution to minimize negative consequences. As an example, if a database is breached, one option is to shut it down. However, business-critical activities might be going on using that database. If that's the case, maybe there is a less obvious but equally effective solution.

Many security breaches, such as a database breach, require immediate responses. In these cases, security teams will act as quickly as possible. If they don't have the proper context though, the solution could end up being worse than the problem.

This brings us back to the silo issue. With security teams only seeing what's in their respective silos, security responses can be slow, ineffective, inefficient, and ultimately disruptive.

REMEMBER

When it comes to security, context means a lot. Context, context, context!

IN THIS CHAPTER

- » Consolidating detection analytics
- » Investigation remediation
- » Benefits of orchestration and automation

Chapter 3
XDR: Integrating the Security Stack

A disjointed security stack can lead to a lot of trouble. Security professionals often lack the context they need to confront security issues quickly and efficiently, alert fatigue means valid security concerns go unattended, and security staff are overworked chasing down false positives.

Extended detection and response (XDR) solutions provide many benefits, but one of the most important is how they attempt to integrate the security stack. Analytics, remediation, and automated tasks become streamlined when allowed to access and understand the full context of your security stack. This chapter examines how XDR brings it together.

Detection Analytics

Detection analytics isn't just about what you're seeing; it's also about what you're learning. Successful security operations (SecOps) involves dealing with a threat and figuring out how to deal with similar threats in the future. That often involves more than looking for software vulnerabilities similar to what you've seen in the past or thinking in terms of how a specific piece of malware could infect your system again.

TIP

Seeing attack patterns and strategies used by attackers is powerful information. Both the kinds of attacks and the methods of attacking are changing. Good detection analytics tries to deal with both.

The detection analytics capabilities of XDR platforms are founded on integration. Here are the main sources XDR is looking at and aggregating:

- **Endpoints:** This includes employee workstations, laptops, smartphones, tablets, IoT devices, and more.
- **Networks:** This includes public and private networks, virtual private clouds, and more.
- **Applications:** This includes email, and any software as a service (SaaS) used by staff, such as access through a web browser.
- **Cloud:** Cloud services can include cloud databases, management tools, and more.

XDR lets security teams see all these parts together — how they talk to each other, what went where, and so on. Let's take a look at how this integration changes what security teams can see and how they operate.

Aggregated threat intelligence and visualizations

A key feature of many XDR solutions is an aggregated view of threat information. What this looks like changes from platform to platform, but the heart of it is readable visualizations of relevant security information in the event of a security issue.

Because XDR reaches from endpoint to security team, the platform can show security pros an end-to-end view of the problem. Look at the endpoint — or points — that might be the breach point, see the alerts that brought it to your attention, which resources the attack could be impacting, and more.

REMEMBER

XDR platforms look at so much information and can organize it in an accessible way, that aggregating threat intelligence in this context is almost a real-time audit. You get to see the relevant security information just after the event has happened.

How all this information is shown to security staff depends on the XDR platform, but there are some common methods of visualizing security info:

- **Dashboards:** Many platforms have a dashboard that can be fitted with different security information sources, for easy reference and monitoring.
- **Threat maps:** XDR platforms often have infrastructure visualization tools that allow you to see the relationships among services or resources. This may be a node graph, a map, or some other representation of relevant security information.
- **Customization:** XDR platforms often provide customization options for how and where all these resources are represented.

TIP

Different organizations require different things out of their security solutions, so flexible monitoring and threat intelligence is a must. Dashboard components often visualize security issues over time. For instance, line graphs displaying the number of network penetration attempts over the last six months, or response times for malware detection and remediation.

The mapping capabilities of XDR allow security teams to see a breach from end to end — where it started to where it is now — and what it could potentially affect along the way. This point is so important that it's about to get its own section!

Correlating and contextualizing

Context and correlation visibility are XDR's not-so-secret weapons. Before we get into it, here are working definitions of the terms within the IT security space:

- **Context** helps answer the "why" of a security issue. Ideally, it puts security problems into a full-stack perspective, showing the potential ramifications of an attack or a solution.

- **Correlation** should answer the "where" of a security issue. It's about which resources are being affected and what those compromised resources may, in turn, impact.

XDR platforms focus on the endpoint and work their way in from there, so the security tools that make up the ecosystem will be visible. Without a clear view of the full scope of an attack — from endpoint to network to applications — threat assessment and remediation suffers. There are three main reasons that current IT security breaches are so challenging:

- The number of potential attack points has increased in recent years.
- The complexity and sophistication of attacks has grown.
- In response to these new challenges, security stacks have also gotten more complicated.

One of the key ways XDR platforms help security teams deal with these new challenges is through visualization. XDR threat mapping features show the correlation between disparate systems involved, directly or indirectly, in an attack. For instance, a piece of malware is found. Using a threat map, the malicious software is traced back to an endpoint laptop, where an employee opened an attacker's email.

What about a context example? Say there's a large scheduled input/output spike in the middle of the night: A simple alert trigger won't have full context. This alert might be triggered simply because it seems like suspicious behavior, when it is, in fact, a business-critical operation. With a broader context, security teams, and their alert systems, will know more about why things are happening. False positive threats are time and energy drains and can even lead to teams missing legitimate threats due to alert fatigue.

So, correlation and contextualization capabilities show security teams the big picture. The next question is: What do you do about what you see?

Identifying threats and formulating a response

Thanks to XDR-fueled correlation and context, threats are easier to identify. XDR cuts down on the time to find the location and larger implications of an attack, but it's also directly impacting how security professionals go about dealing with a threat.

First, XDR's full-stack approach, along with the extensive security histories teams can build up, means anomalies can be identified as anomalies.

An activity bump on Server A, followed by a bump on Server B, might be regular business activity. It's a pattern that can be recognized by your security systems working in tandem, and this information can be applied to future attacks. What if Server B sees an activity bump but Server A is quiet? XDR will recognize this as anomalous behavior and trigger a response.

Analytics speeds up response formulation, too. Examine the compromised Server B again. Server B may be running a piece of software that has a known vulnerability. Because the security team has identified this server as the problem area, they can quickly search for known vulnerabilities in this software and patch it as needed.

Detection analytics also helps security teams respond smarter, not just faster. Server B, while it is being attacked, might be feeding business-critical data to Server C. Because of this, Server B can't be shut down or interrupted. Security staff know this because they have the full picture, and they can formulate a new plan that doesn't interrupt important business operations.

Investigation Remediation

You can find threats all day, but it doesn't mean much if you don't take care of them. There are many approaches to remediation, and XDR tries to help ease the burden of finding the right one and enacting it.

REMEMBER

There are two primary ways XDR improves investigation remediation: supporting security operations center (SOC) staff and giving a boost to incident-tracking capabilities.

SOC staff are often overworked, and there are security consequences to this. XDR can lighten the load by streamlining and simplifying many necessary security operations. Incident tracking is greatly improved with what XDR brings to the table as well.

Attack history tracking has security implications that can be great tools for security teams.

Support for SOC

SOC staff have to work hard and fast to keep up with the current threat landscape. Many security tools haven't caught up to SOC's practical needs, unfortunately. Not only does an inefficient security stack add stress to security teams, but it can also induce alert fatigue that leads to missed threats.

XDR brings multiple types of benefits beginning with support for preparing for security incidents, starting with the ability to analyze and understand protected resources, such as applications, endpoints, and data servers. XDR's detection capabilities address one of the most difficult aspects of security management with a combination of continuous analysis and up-to-date threat intelligence. Once a threat has been detected, the SOC can use XDR tools to contain the threat by segmenting to prevent malicious content from infecting other resources. The analysis provided by XDR is crucial for eradication and recovery from attack. For example, an attack may exploit an unpatched device that must be identified and patched as part of the recovery process. XDR also supports post-incident analysis with information related to root cause analysis, identifying vulnerabilities, and adjustments to processes and procedures.

TIP

This makes it sound like alert fatigue might turn into dashboard fatigue, but the customizability of these central views should prevent that from happening. You only need to line up what you need to see.

Custom analytics tools give context to a security issue, meaning an easier time prioritizing incident responses, a reduction in false positives, and more efficient SOC operations.

Another important set of tools XDR brings to the table, from an SOC perspective, is orchestration automation. SOC staff are proficient, well-trained security professionals, and bogging them down with tasks that could be automated is just a waste of their valuable time.

An endpoint laptop that is compromised can be quickly locked out of your network given the right automation triggers. The time it would take a human to carry this out would be both slower, and better spent somewhere else. The human side of things, when possible, should start when the difficult planning and decision-making is needed.

REMEMBER

Automation isn't just about saving time. It's also a way to speed up the entire response process.

Incident tracking

Another blessing for remediation security teams: attack histories. XDR platforms include customizable dashboard modules, or sometimes dedicated dashboards, for tracking and logging past security breaches. This is sometimes tracked per system, such as by listing database breaches and network attacks separately, or by type of attack, such as listing all DDoS attacks.

Attack pattern recognition gives useful insights into future attacks. If a breach is identified and is displaying behavior teams have seen before — maybe many times before — they will have a much easier time dealing with the threat.

Having a history of past attacks is a way to build institutional knowledge about common attack types and patterns. It is important to correlate threat intelligence from both internal and external sources in your historical view and include appropriate expiration dates for that intelligence, especially in the case of IPs, which can transfer ownership easily and leave a critical resource on the "block list." SOC teams can identify common threats faster, and respond to them more efficiently, with the body of knowledge security teams built themselves.

Going back to the forever-doomed Server B example, say the activity spike on Server B is identified as a threat. Security teams, using knowledge from attack histories, might recognize the kind of activity going on, its preceding and current patterns, and know exactly what kind of attack it is, as well as have a good idea where it's coming from.

This kind of historical information extends to responses themselves. If this kind of attack has happened before, then security teams have dealt with it before. Tracking incidents should be more than just identifying issues: It should also include figuring out how to better deal with these issues in the future.

TIP

When attackers give you malware, make lemonade. Squeeze every ounce of information out of security breach histories. Attacks are bad while they're happening, but they turn into a powerful security resource.

Orchestration Automation

Orchestration automation is how XDR platforms support automating jobs that may require information from across the security stack. It involves integrating disparate security tools so automation tasks can benefit from the different security vantage points, as well as carrying out the actual automation jobs.

Integrating multiple security technologies

The pile of security tools that make up a security stack is complicated; however, integrating them through XDR can simplify automation scripts and jobs. Like many other parts of SOC tasks, lack of context makes life a lot harder for automation. A full-stack view lets automation tasks have more complex, sophisticated triggers that respond more efficiently and consistently to legitimate threats.

Automation within a siloed endpoint solution might only catch a portion of endpoint breaches, without information about network security and incident response logging. Leveraging orchestration capabilities only increases the effectiveness of security responses across the stack.

TIP

Don't make the solution worse than the problem. Avoid custom, ad hoc scripts for each new response. Security professionals shouldn't have to add software maintenance to their list of responsibilities.

There is also the matter of taking care of the automation scripts themselves. Automation tasks in siloed environments frequently need babysitting. Software updates, compliance changes, and security tool changes can all interrupt the regular use of ad hoc scripts.

Having integrated security tools available for automation tasks means security teams can utilize more information and a more stable environment. Edge cases with custom automation scripts can be integrated into a larger automation solution, which means less babysitting and fewer scripts for you to track.

REMEMBER

Ad hoc automation isn't automation!

Automated responses

You've got the integration and the scope, but what can automation actually do?

With XDR, security teams can make more fine-grained automation tasks than other kinds of security solutions might allow. The security stack scope and attack histories mean XDR automation tasks are well-informed blueprints for how attacks will be carried out.

Take a look at an endpoint example: An endpoint has been identified to have malware running on it. An automation task, built up by security staff to respond to this kind of threat, has a specific series of actions it carries out, to make a preliminary pass at remediation. In this instance, it might include isolating the endpoint from the rest of the network, then running antimalware software on the infected machine.

In the case of a data breach, there may be a more complex set of automated responses needed to properly deal with it. Some databases can't be simply shut down because they might be involved in business-critical tasks. Instead, an automated response could, given certain criteria, decide a breached database can't be shut down and instead change a firewall rule to stop data egress from that server.

IN THIS CHAPTER

- What is SIEM and where is it looking?
- What is SOAR and what is it doing?
- How SIEM and SOAR interact with XDR

Chapter 4
XDR, SIEM, SOAR: Friends or Foes?

We can't talk about extended detection and response (XDR) without also going over its two biggest predecessors: security information and event management (SIEM) and security orchestration automation and response (SOAR). They're two of the most prominent security tools on the market that advertise themselves as big-picture problem solvers.

SIEM and SOAR take different approaches to strengthening the IT security stack and provide different outcomes for the customer. While their spaces are being encroached upon by XDR, the old standards aren't wholly incompatible with the new kid.

SIEM

Security information and event management (SIEM) is a security solution that focuses on gathering security data from across a security infrastructure and providing as many logs and alerts as possible. This concentration on raw security information has pros and cons.

REMEMBER

On the one hand, piles and piles of logs are sometimes exactly what your organization needs. Compliance-heavy industries, such as healthcare or finance, often need large amounts of data about their internal systems. On the other hand, many industries simply don't need to know about every single blip on the security radar. Many times, these blips aren't attacks. The following sections go through some of the capabilities of SIEM solutions and what they mean for security teams.

Where is it looking?

The short version is that SIEM solutions look where they're told to look. As the product type has evolved, SIEMs have gotten better and better at gathering information and putting it into a central location for analysis. SIEM's data-collection capabilities are reliant on the products and tools it's monitoring.

SIEM is a tried-and-true security tool that attempts to integrate previously siloed systems that need monitoring. Here are some of the locations SIEM tools can monitor:

- Firewall events
- IoT devices
- Security devices
- Endpoint detection and response (EDR)
- Applications

Event logs are collected in a centralized location for processing and analysis. Recent additions to the SIEM realm have added some automated processing features, orchestration tools, and other capabilities that have been exclusive to SOAR solutions.

SIEM solutions use different rule-based systems to determine whether activity on the monitored resources is suspicious. If behavior is determined to be potentially a security breach, alerts are sent to a central access point for security staff to go over and decide on a course of action.

SIEM has been around for a while and has proved its usefulness repeatedly. However, there are some limitations to this kind of security solution, which newer solutions are overcoming, while keeping the main benefits of SIEM.

The outcome is limited visibility

SIEM's ability to manage an entire security stack's worth of alerts can be a powerful tool. It can also, counterintuitively, lead to less visibility of the entire ecosystem for security teams. Alert fatigue and false positives put unnecessary stress on security staff and can lead to missing legitimate threats.

Alert fatigue is the result of a security system outputting so many security alerts that security teams become overwhelmed with checking the validity of the threats. There are a few reasons too many alerts could be coming through:

- Siloed systems cause security teams to misunderstand which behavior is actually suspicious.
- The alerts don't have enough context to be accurate.
- The alert system itself doesn't provide the fine-grained alert control necessary to tailor alerts to specific needs.

When alert fatigue sets in, security teams are more likely to miss threats that do need to be dealt with. They're too preoccupied with unnecessary alerts that are burying legitimate security issues.

Siloed systems and broad alert criteria also lead to security event false positives. Without the context of the larger IT ecosystem, alert tools will often misrepresent what is happening in the systems or falsely identify security threats. A server may see a spike of activity over a holiday weekend that triggers an alert for suspicious behavior when this activity is a planned job that should be running during non-peak hours.

False positives are a waste of security teams' time and add to alert fatigue. This can create a culture of expecting an alert to be low priority, as it probably won't be a real threat. Alerts should be taken seriously and provide teams with information they need to know.

REMEMBER

Quality over quantity. Security teams need good information, not lots of it.

SOAR

Security orchestration automation and response (SOAR) solutions are more on the preparation and action side of security and, at first glance, seem quite similar to XDR platforms. The main difference between the two is integration, which affects what security teams can do and how they do it.

What is it doing?

SOAR solutions aim to streamline orchestration and response through automation tools. SOAR is a security tool category that is relatively new to the IT landscape — coined by Gartner in 2017 — and has provided adopters with new ways to deal with threats.

The core of SOAR platforms is the "playbook." This is an orchestration tool that is designed by security teams to plan a sequence of actions in response to a threat. Parts of this plan may be streamlined through automation, which can often use machine learning techniques to improve performance.

SOAR solutions can't stand on their own, however, so they offer integration with other security tools such as network detection and response (NDR) solutions. SOAR can then respond to the information generated by the other tools using playbooks and automated functions.

These platforms are powerful tools for orchestrating security responses, but there are some drawbacks. While they do offer integration with other security tools, SOAR platforms often make it a hassle to get them up and running and suffer from a lack of comprehensive detection capabilities.

The outcome is SecOps burden

Security operations (SecOps) teams take on the job of securing business resources and systems. Networks, applications, and customer and business data all fall under their watchful eyes. This is a lot to keep track of, and SecOps teams don't need extra weight slowing their work.

SOAR solutions often have integration compatibility with many kinds of security tools, many of which will already be part of your security infrastructure, but there is sometimes extra work involved to get SOAR friendly with the other tools. Many SOARs have lackluster API access, meaning fully integrating the security observation tools you need is difficult, if not impossible.

This challenge can lead to workflow interruptions, detection limitations, and the need for extra security tools to fill in the gaps. All three of these factors cause SecOps teams to work harder and less efficiently. Each new tool in the security stack is a new point of failure, a new solution to integrate and learn, and a new burden for the already busy professional that has to watch over it.

REMEMBER

Although SOAR is a powerful security tool, it can add headaches to SecOps that aren't necessary. This is especially the case with the recent advancements in XDR platform capabilities.

Putting It All Together

Like SIEM and SOAR, XDR can't stand on its own. It requires other security tools to support it, give it the information it needs to function, and fill in the gaps in its feature set. Both SIEM and SOAR are competent security solutions and have proven to be useful for many organizations. XDR is new and promising, but the more established tools shouldn't be discarded and forgotten.

SIEM and SOAR feed into XDR

XDR offers a lot to organizations, but it is not a cure-all. A successful XDR deployment needs other security tools to back it up and, depending on the specific needs of an organization, could benefit from integrating the strengths of SIEM or SOAR solutions with their XDR.

With SIEM being such a strong tool for logging and alerting, it can bolster XDR analytics capabilities by providing comprehensive log data. Since XDR can handle large amounts of security information, a deluge of SIEM logs shouldn't lead to critical information loss or missed alerts. SIEM solutions could also help teams using XDR to strengthen their compliance requirements. Some organizations simply require large piles of logs to meet industry standards, and XDR can be the analytics and organization tool needed to deal with it.

SOAR integration with XDR is more of an edge case, however. XDR solutions offer comprehensive orchestration and automation tools, which is exactly SOAR's big selling point. XDR can be used for its analytics and tools, though, while an accompanying SOAR solution is used for many of the automation and orchestration tasks. This is an option for those who simply like using the SOAR product already used in their security environment. SOAR's playbook and automation capabilities might be what your security teams want to stick with, and they can instead benefit from XDR's analytics and centralized viewpoint without taking advantage of its other tools.

REMEMBER

XDR shouldn't be seen as purely a replacement for existing security solutions, but a welcome addition to the security landscape. There are instances where XDR can replace existing tools, but one of the strengths of the product type is its capability to integrate with security environments that already exist.

Centralizing security information

One of the ways that XDR is able to integrate so effectively with existing security infrastructure is through its focus on centralizing security information. Here are a few features that enable XDR to centralize what security teams need to see:

- **Customizable dashboard:** XDR solutions often have at least one central dashboard with customizable observation panes. These areas can be moved around to show different portions of your security infrastructure, alerts, attack histories, and more.
- **Incident maps:** These are visualizations of security incidents that show which systems an attack impacted and what else it may have come into contact with. It's akin to epidemiological maps used to study disease spread and can help teams trace an attack to its source.
- **Access to supporting security tools:** Most XDR solutions provide easy access to the other security tools feeding the platform information. This usually shows up as part of the central dashboard or a quickly accessible menu.

XDR's big integration promises wouldn't be much without a centralized way to access all that information, so XDR vendors are keen to make their products easy to read and use. Centralized information reduces workloads on security teams, reduces identification and response times, and gives security pros the space to improve future responses instead of digging through swaths of data.

Other Technologies to Be Aware of

Two technologies to consider when thinking about XDR are endpoint detection and response (EDR) and network detection and response (NDR). These two tools can act as great support tools for a successful XDR deployment, by helping security teams navigate the complexities of network and endpoint environments.

EDR, sometimes called endpoint threat detection and response or ETDR, can be thought of as a relative or precursor to XDR. It performs some of the main functions of an XDR product, such as focusing on endpoint monitoring and detection, although it usually doesn't have many of the centralized viewpoint and analytics capabilities of XDR platforms. EDR is important to keep in mind because it's likely the right kind of tool for feeding your centralized XDR solution the endpoint security data it needs.

NDR is similar to EDR, but instead it monitors network activity and resources. NDR can help identify network threats and perform automated responses although, again, these solutions don't often have the comprehensive tools provided by XDR. The advantage of having a dedicated network security monitoring tool is that you need visibility into attacks on networks, which are becoming more complex and multipronged. There are often multiple points of attack, and a laser-focused network security tool can add a lot to a security infrastructure.

REMEMBER

XDR isn't a bully that has come to steal your SIEM's lunch money! It's a platform that plays nice with many security tools you're already using.

IN THIS CHAPTER

- » **Cisco's XDR philosophy**
- » **Breaking down the Cisco XDR platform**

Chapter 5
Cisco's Approach to XDR

Cisco takes a unique approach to extended detection and response (XDR), through a set of patented tools, multiple machine learning techniques for data analysis, and automation capabilities, which are suitable not just for speeding response times, but also for proactively dealing with potential security issues and more.

Cisco XDR combines AI with threat detection and response technologies to simplify security operations and accelerate SOC teams' responses to security incidents. Today's security threats are increasingly sophisticated and designed to minimize the chance of detection. In response to this, Cisco has created an XDR platform that correlates data from endpoint, network, firewall, email, identity, and DNS systems giving SOC teams a comprehensive view of their systems and the capability to respond quickly to isolate and mitigate active threats.

Three Pillars of Effective XDR

Cisco Secure sees XDR as a security platform that fails if any of its component parts isn't doing what it's meant to do. The "extended" in XDR doesn't do much if there isn't a powerful analytics toolset to leverage it, after all. Each of the three main parts of the XDR platform have to work in tandem to deliver the big promises of this new approach to IT security. This section covers the three pillars of Cisco XDR philosophy.

X: A broad reach

The extended reach of XDR not only lets security teams see more, faster, but also helps simplify the unwieldy and complex modern security stacks. XDR can't do this on its own, so compatibility with existing security solutions is critical to achieving a full view of security resources.

Cisco Secure offers an array of security tools that easily integrate into its platform, and they think this should be the standard. Any XDR platform worth using should have broad integration capabilities so organizations can get the most out of the tools they already have, while still benefitting from an XDR platform.

Additionally, an XDR platform should be pulling data from as many sources as it can. Any resource or endpoint that has information to collect is a potential attack point and has to be monitored. A good XDR platform should have full compatibility with strong network detection and response (NDR) and endpoint detection and response (EDR), ensuring full visibility of all vulnerable resources.

D: Fast, powerful analytics

An equally important part of XDR is how it enables security staff to correctly identify and learn from attacks. There are two main components of XDR analytics: 1) how the information is processed by existing tools and XDR artificial intelligence (AI)/machine learning tools, and 2) how the information is presented to security teams.

The complexity of current IT environments means there is a lot of security data that requires context to fully understand and act upon. AI-powered analytics tools are the most efficient way to process this amount of data, and a good XDR solution should include powerful machine learning capabilities to support security teams.

REMEMBER

Security information readability is also a must for a successful XDR solution. This includes easy-to-use dashboards that hold the information you need, when you need it, and visualization tools to better analyze security data.

Visualization should include attack histories, usage metrics, network activity, and the capability to map out a threat's points of contact with your systems. XDR analytics are about fast, accurate threat identification so security professionals can quickly get to solving the problem at hand.

R: Reducing dwell time through automation

Automation has been a part of the IT security space for some time, but XDR platforms can take it to a new level. Automation as part of an XDR platform benefits from the solution's other strengths. Automation plans are well-informed, they have access to a full security stack of insight, and can be easily managed through a centralized dashboard.

REMEMBER

Not only do these benefits reduce security staff workloads, they can also reduce dwell time. Automated responses can get the response ball rolling by isolating compromised resources, shutting down servers, and performing other simple tasks. Because XDR has centralized access to many services, when a threat is identified, automation tasks can prevent similar systems from suffering the same attack. An overarching benefit of automation is that it helps reduce human error, especially when performing repetitive tasks. This can help avoid introducing misconfigurations or other vulnerabilities when performing required security operations.

Cisco XDR Platform

Cisco XDR is a cloud-native, built-in platform experience within Cisco's portfolio and connected to your infrastructure. The platform shifts SOC teams' focus from long-running investigations and data analysis to remediations. The platform is integrated and open for simplicity, unified in one location for visibility, and it maximizes operational efficiency to secure your endpoint, network, firewall, email, and identity. It reduces dwell time and human-powered tasks to counter attacks and stay compliant.

Integration with new and existing solutions

A good XDR product can't be locked out of certain systems due to lack of solution integration. As such, Cisco XDR maintains an open stance toward other security products that have open and robust RESTful APIs, many of them integral in taking advantage of XDR's full potential.

Many SIEM and EDR solutions suffer from poor integrations. This in turn, leads to vendor lock-in and an inability to aggregate and correlate data across solutions, resulting in extended times to investigate and remediate incidents. The longer a threat is active, the greater the impact. Integration across systems is essential to quickly addressing threats. This is why Cisco XDR is designed to ingest, integrate, and correlate a wide variety of data from different systems and applications.

Cisco is committed to long-term support of integration with third party security solutions with a range of curated and supported integrations.

Unified Detection

With the unified detection capabilities of Cisco XDR, SOC teams are able to rapidly:

- Correlate data across telemetry points regardless of vector or vendor
- Apply Cisco Talos intelligence, machine learning, and other AI methods to enrich data for better detection
- Prioritize incident response based on evidence discovered in the correlated data sets assembled and analyzed by Cisco XDR

REMEMBER

It’s one of the primary components of XDR that allows security staff to identify and respond to threats quickly. Centralized views of a security ecosystem can help reduce alert fatigue and information overload as well as reduce false positives by providing clear, accurate information to security teams.

Threat detection and response

When combined with the detection capabilities of Cisco Secure products, Cisco XDR’s threat detection and response features include a multilayered approach to machine learning analytics. Several machine learning engines — including supervised, unsupervised, statistical, and behavioral — make alerting and identification fast. These engines cross-reference threat behavior with existing security knowledge to aid in prioritization and to jump-start a response plan.

Security information is given context within the larger ecosystem, and teams can see correlations between impacted resources and systems. Cisco XDR benefits greatly from the telemetry gathered from Cisco’s large customer base in this regard. Cisco takes advantage of a global threat intelligence network that can identify threats and quickly identify future instances of that threat across its customer base. Powerful analytics, the centralized view, broad threat intelligence, and easy access to security resources means response times can go down and security teams have the room to make more informed decisions about how to respond.

Automation

The security skills gap is well known in security. Finding skilled security professionals and helping them continuously develop their skills is a common challenge. One way to address this skill shortage is to employ automation.

With automation, SOC analysts can take responses that coordinate actions across security tools without requiring deep and detailed knowledge of all the tools involved. Automation and guided workflows are key to enabling analysts to take fast, decisive actions. This kind of workflow also provides progressive disclosure that reduces information overload by providing information in context at the right time. Automated responses, approvals, and action can be incorporated into a response playbook to speed response to future security threats.

Support for automation extends from the ingestion and integration of data through analysis and response. By correlating data from multiple sources, Cisco XDR has the data it needs to extract facts about the security state of complicated environments. These assessments provide the evidence needed to apply further analysis techniques to determine the most appropriate response to an incident. In addition, automation in Cisco XDR continues with support for incident response.

Chapter 6
Ten Things to Remember about XDR

This chapter discusses some of the big takeaways from this book, and highlights key features to look for in extended detection and response (XDR) solutions and comprehensive security platforms.

Reduce Time to Detect and Respond

At the end of the day, XDR platforms aim to reduce detection and response times. More data and more tools don't mean faster security teams. They often mean overwhelmed security teams. XDR focuses on providing actionable information through machine learning-supported analytics and a centralized dashboard. On the response side, orchestration and automation features streamline the response process by providing easy-to-use and customizable tools for security staff.

Visualize Integrated Security Data

XDR takes in a lot of information and must organize it to reduce alert fatigue, false positives, and general security operations hassle. Central dashboards are customizable information hubs for security teams to organize their data to fit the organization's needs. Visualization tools such as incident maps should help identify threat sources and trace potentially new attack points.

Precise Monitoring

Because XDR platforms usually come with machine learning-based analytics, and rely on secondary security tools for data collection, security teams should have a clear view of an organization's ecosystem. Providing good information, over lots of information, cleans up what staff actually see, making it easier to focus on legitimate security concerns.

Contextualize Alerts and Reduce False Positives

XDR's centralized dashboard features provide context to security situations. Alerts coming in are more reliable because the XDR system has the relevant threat intelligence required to make decisions about what is concerning abnormal behavior and what isn't.

False positives are a waste of resources, and XDR's comprehensive view of the IT infrastructure helps reduce their frequency.

Automated Responses

Automation features have been around in the security space for some time, but XDR's broad reach enables its automation tools to benefit from some fine-tuning. Many XDR products offer machine learning-supported automation that can take care of rote security tasks, so security staff can work on the harder jobs that need human intervention.

Keep It Open

XDR isn't a lone wolf and needs the support of specialized security tools. XDR platforms offer a lot of integration options, both with existing security tools and ones that may be added in the future.

TIP

EDR and NDR in particular are two tools to think about including when building out your security infrastructure.

Store and Analyze Logs at Scale

Because of the powerful analytics tools XDR brings in, these platforms are able to process large amounts of security data. XDR solutions are easily scalable so your organization can grow over time, without worrying how your security analytics will have to change.

Address Compliance Requirements

The large amount of data that can be processed by XDR also means compliance and industry regulation requirements can be confidently met.

REMEMBER

Organizations involved in healthcare or finance are especially in need of extensive logging and analysis tools.

Siloed Solutions Are Partial Solutions

Security infrastructure has become so vast that siloing systems has become common. Enterprise-level IT infrastructure can't rely on this separation of systems, as attackers expand and develop their attack strategies. Incomplete security information can lead to false positives and alert fatigue, because monitoring tools won't have the full context of suspicious activity.

Remember the Human Factors

The security personnel managing these tools are the most important part of any successful IT security environment. Inefficient security solutions overwork security staff by burdening them with false positive threats, unnecessary alerts that lead to alert fatigue, and lackluster identification and response tools that slow them down.

Get a centralized viewpoint of your security infrastructure!

The primary goal of XDR platforms is to reduce detection and response times, minimize alert fatigue, and add context to legitimate alerts. XDR focuses on providing threat intelligence through machine learning-supported analytics and a centralized dashboard that enable you to act on threats with confidence. Orchestration and automation features streamline the response process by providing easy-to-use and customizable tools for security staff.

Inside…

- How security threats have evolved
- Modern security tools and techniques
- Breaking down XDR
- How siloed solutions create roadblocks
- Overcoming the problems faced by enterprise security operations
- Consolidating detection analytics
- Investigation remediation

CISCO

James Sullivan is a technology writer based in Portland, Oregon. His work is concentrated on cloud security, IoT, and cloud database solutions. **Dan Sullivan** is an enterprise architect specializing in data architecture, analytics, data mining, statistics, and computational biology.

ISBN: 978-1-394-26618-0
Not For Resale

9 781394 266180

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT