5 Ways to Experience XDR

Preface

In today’s rapidly evolving world, dealing with cybersecurity incidents effectively is more critical than ever before.

An incident management program is crucial for a Security Operations Center (SOC) as it provides structure, efficiency, and efficacy in handling security incidents and ultimately enhances the organization's ability to protect its assets and mitigate potential risks.

An effective incident management program should provide the following five benefits:

1

Timely response enabling the SOC to promptly detect, analyze, and respond to security incidents. By ensuring incidents are addressed promptly, SOC teams minimize the potential impact and reduce the organization's overall risk.

2

Efficient coordination establishing clear processes and workflows for handling security incidents. Effective coordination among SOC team members allows them to work together seamlessly and efficiently during incident response, when collaboration and communication are most critical to success.

3

Standardized procedures for incident identification, classification, prioritization, and response. This consistency helps SOC teams ensure all incidents are handled in a structured and organized manner, reducing the risk of errors or omissions.

4

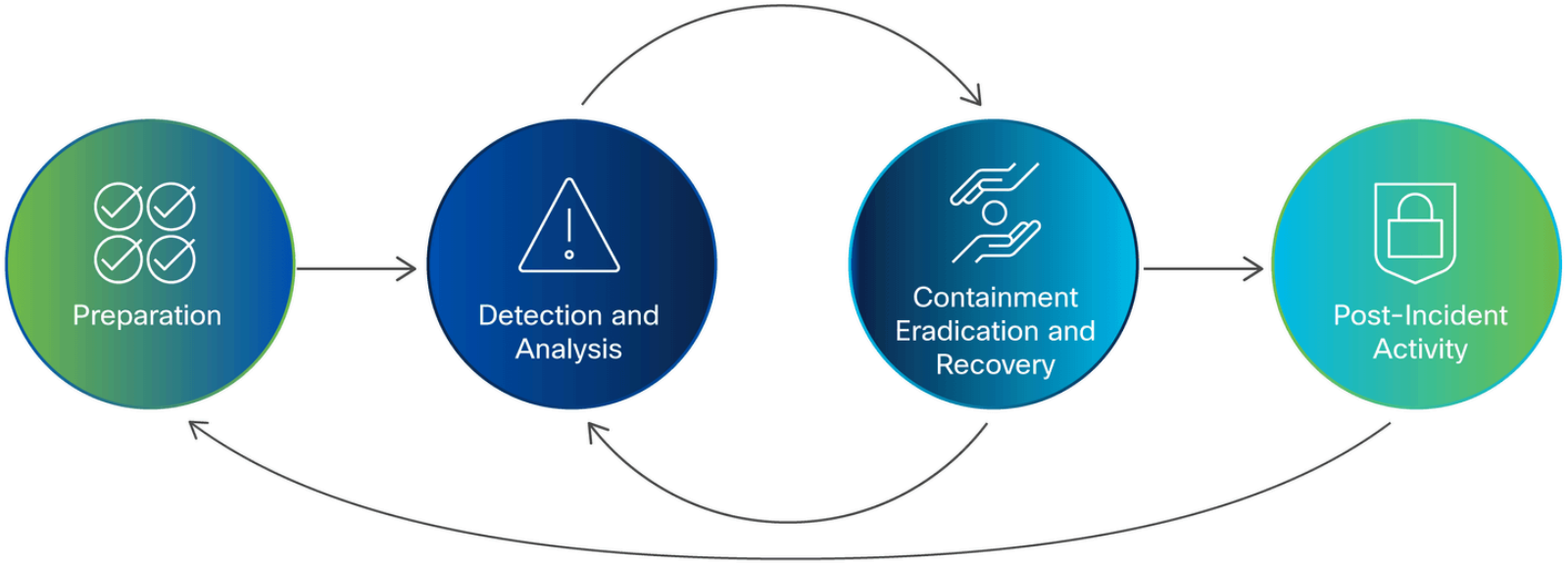
Continuous improvement allowing the SOC to capture valuable data and insights from each security incident. This data can be used for post-incident analysis and lessons learned, enabling analysts to continuously improve their incident response capabilities and enhance their organization's overall security posture.

5

Compliance requirements to cover regulatory frameworks and industry standards that require organizations to have an incident management program in place. By implementing an incident management program, a SOC can demonstrate compliance with these requirements and ensure security incidents are managed in accordance with best practices and legal obligations.

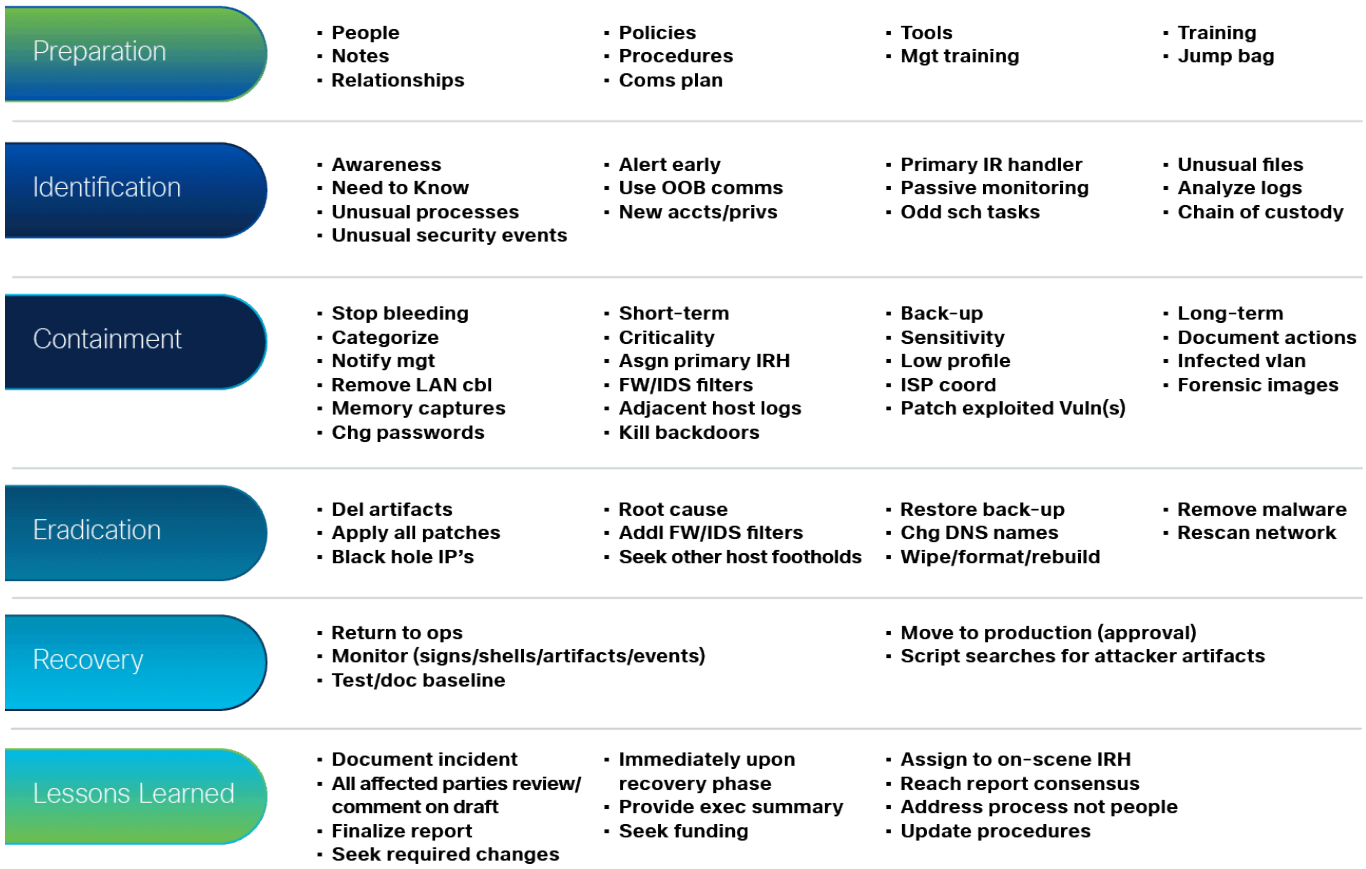
The main goal of an incident response framework is to provide prescriptive guidelines for creating an effective incident management program that can help an organization reduce the impact of security incidents. The PICERL model, which stands for Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned, is a commonly utilized incident response framework. The Computer Security Incident Handling Guide published by the National Institute of Standards and Technology (NIST) and the SANS 504-B Incident Response Cycle Guide published by SysAdmin, Audit, Network and Security Institute (SANS) are based on PICERL model as we can see below.

Using these guidelines, SOC teams can develop or refine an incident management program aligned with best practices, while also providing robust incident management capabilities that prevent, detect, and respond to security incidents quickly and efficiently.



Source: NIST

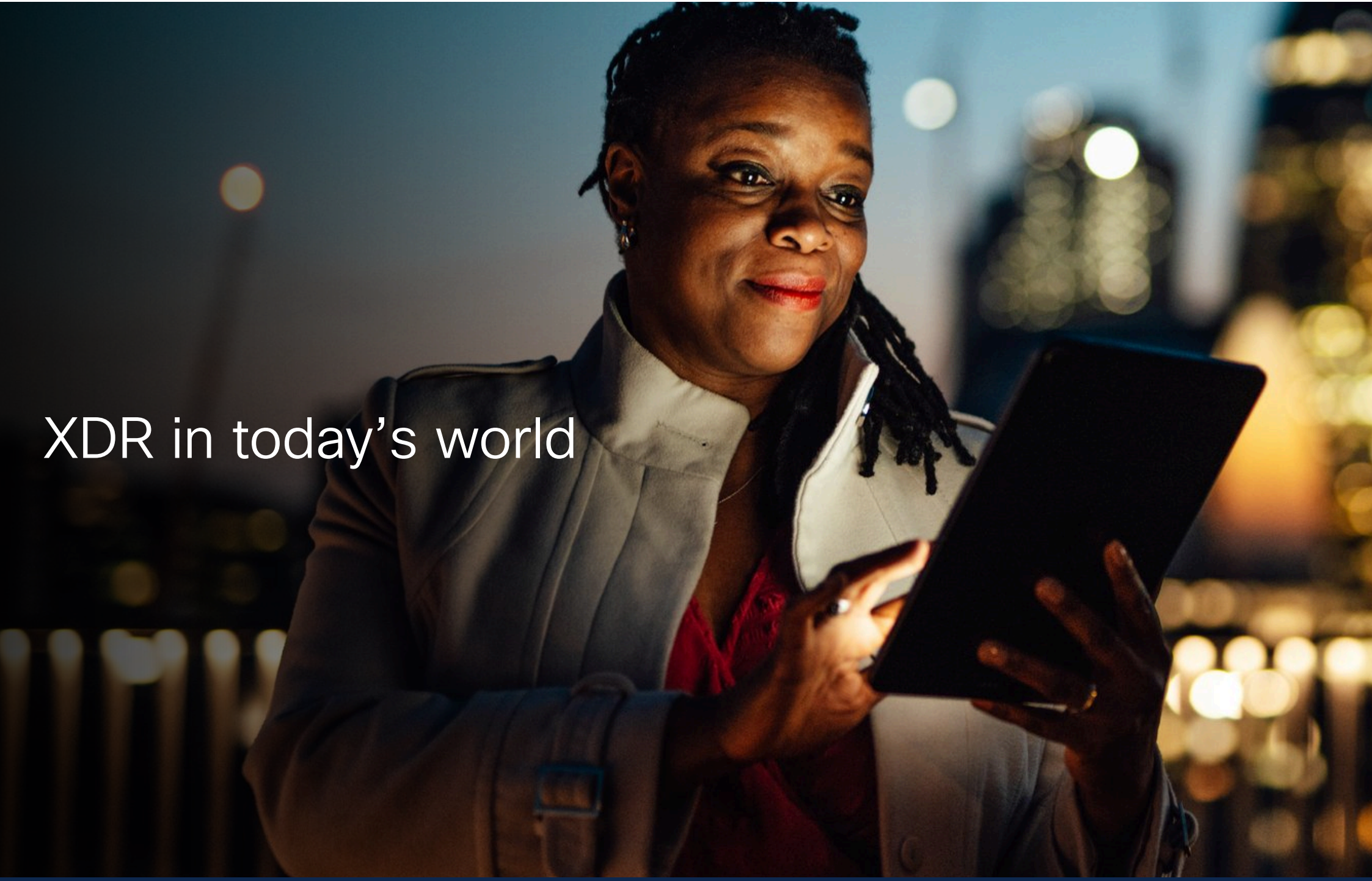
Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)



Source: NIST

An incident response framework provides a structure to support incident response operations. A framework typically provides guidance on what needs to be done but not on how it is done. A framework is also loose and flexible enough to let elements be added or removed as necessary to satisfy a particular organization or constituency.

– David Geer, Geer Communications



XDR in today’s world

The current landscape

An organization's SOC has never been more important than it is today. We live and work in a hybrid, multi-vendor, multi-vector landscape, and if that sounds complicated, it's because it is.

Securing this complex environment is easier said than done, with security teams often forced to operate across dozens of tools with inconsistent integration. At the same time, phishing, malware, and ransomware attacks are becoming more sophisticated and frequent.

The only way to move forward in this new normal is with security resilience – the ability to protect the integrity of every aspect of the organization to withstand unpredictable threats or changes and emerge stronger. And security resilience requires a different security approach than what the past has offered.

Security that meets the moment

With threats becoming increasingly sophisticated, the old detection and response approach doesn't go far enough. Individual security solutions designed to protect different areas of the environment produce a flood of alerts with limited context and fragmented visibility.

This is where Extended Detection and Response (XDR) comes in. XDR is a comprehensive security solution that ingests and correlates data from multiple security tools and sources to provide enhanced threat detection and response capabilities. In the context of a SOC, XDR plays a crucial role in incident response by improving visibility, reducing response time, and enabling proactive threat hunting.

An effective XDR solution must equip a SOC with the following capabilities:

Enhanced visibility

XDR ingests telemetry data from multiple vectors such as endpoints, network, cloud, email, and applications, and enriches it with threat intelligence feeds for accuracy, helping SOC analysts identify and investigate security incidents more effectively.

Faster response time

XDR automates the correlation and analysis of the ingested security data, prioritizing incidents to enable faster detection and response in real-time, mitigating potential threats, and minimizing damage.

Proactive threat hunting

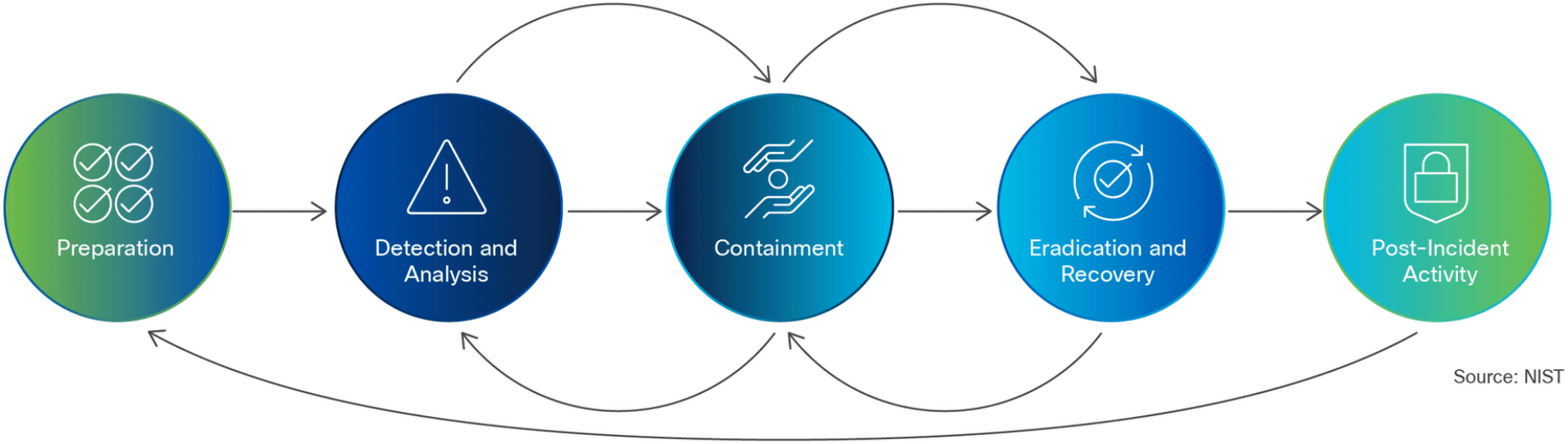
XDR empowers SOC teams to proactively hunt for threats by providing comprehensive visibility across multi-vector telemetry while leveraging advanced threat intelligence solutions to surface threats before they cause damage.

How Cisco XDR aligns to PICERL framework and other leading incident management guidelines

Our goal is to make it easier for your security analysts to secure your organization during all stages of your SOC incident management cycle based on PICERL framework and recommended by NIST under Computer Security Incident Handling Guide Section 3.1 and SANS 504-B Incident Response Cycle.

That's why we've converged capabilities across endpoint, network, email, cloud, and applications into a single solution to deliver the fastest threat detection and response solution on the market today.

Cisco XDR is an open, extensible, cloud-first detection and response solution, built with SOC analysts in mind. Our approach helps you prioritize and respond to threats faster. Cisco XDR ingests, correlates, and analyzes telemetry, providing a single comprehensive view of everything analysts need to quickly detect, investigate, and remediate complex threats across any vector.



Source: NIST

Cisco XDR leverages AI and unsupervised machine learning to detect and respond to threats in real-time. AI helps to automate the detection and response process, freeing up security analysts to focus on more complex tasks.

Additionally, AI improves the accuracy of threat detection by:

- Analyzing large amounts of data, with no need for rules or signatures, to identify unusual patterns or abnormal behaviors that may indicate a security threat.
- Continuously monitoring cross-domain telemetry and alerts originated in network traffic, endpoint processes, email content, user behavior and identity access, just to name a few common data sources.
- Integrating threat intelligence feeds to constantly update and enhance detection capabilities to stay ahead of emerging attack techniques.

Finally, Cisco XDR powered by AI improves the overall efficiency of security operations by reducing the time and resources required to investigate and respond to security incidents.

Our portfolio of leading security products and services is the broadest in the industry, enabling you to increase visibility across your entire environment. With Cisco's multi-vendor and multi-vendor detection your security teams will be able to identify and close security gaps with confidence.

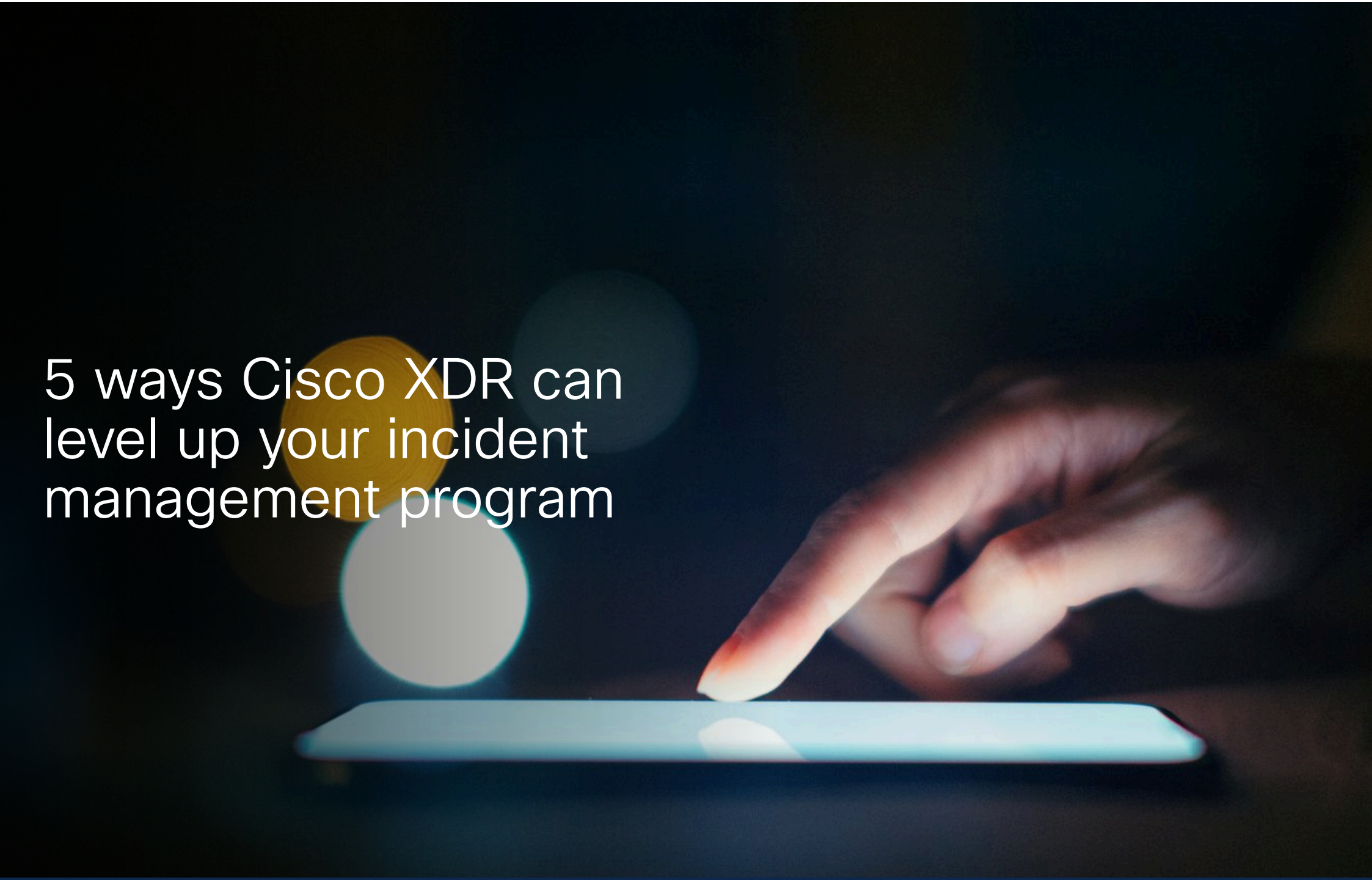
Detect the most sophisticated threats across all vendors and vectors

Act on what truly matters, faster with Cisco's risk-centric approach and prioritized alerts

Elevate productivity with guided remediation, automation, and orchestration capabilities

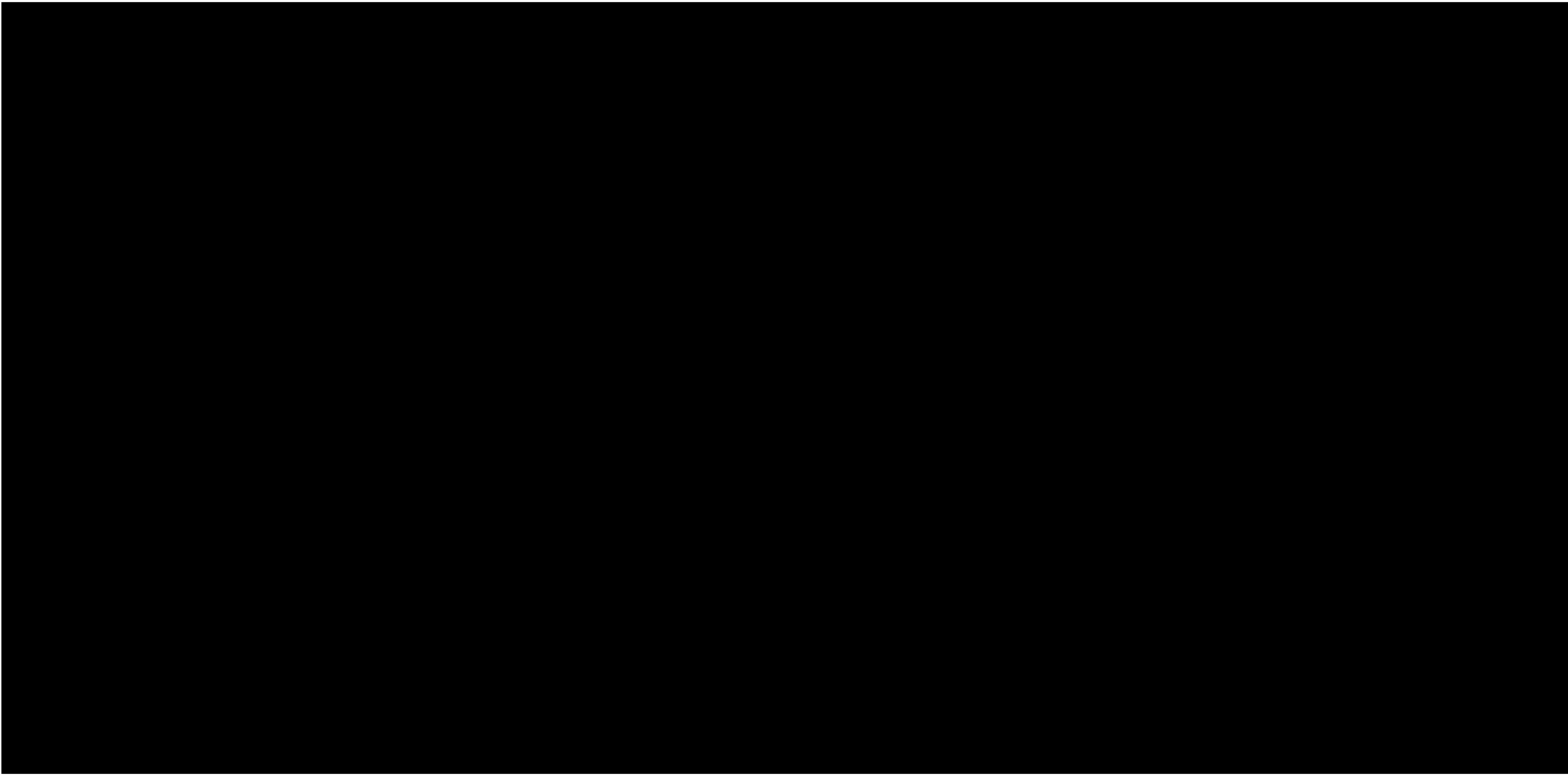
Build resilience by using leading threat intelligence to close security gaps and better prepare for future threats

5 ways Cisco XDR can level up your incident management program



Phishing attack progression

Let’s walk through a frequent phishing attack



Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources.

NIST 800-61 Rev 2 Computer Security Incident Handling Guide

Leverage XDR use cases across incident management stages

Now, let's see how SOC teams can improve their security practices leveraging the new Cisco XDR approach across all stages of a SOC incident management program.

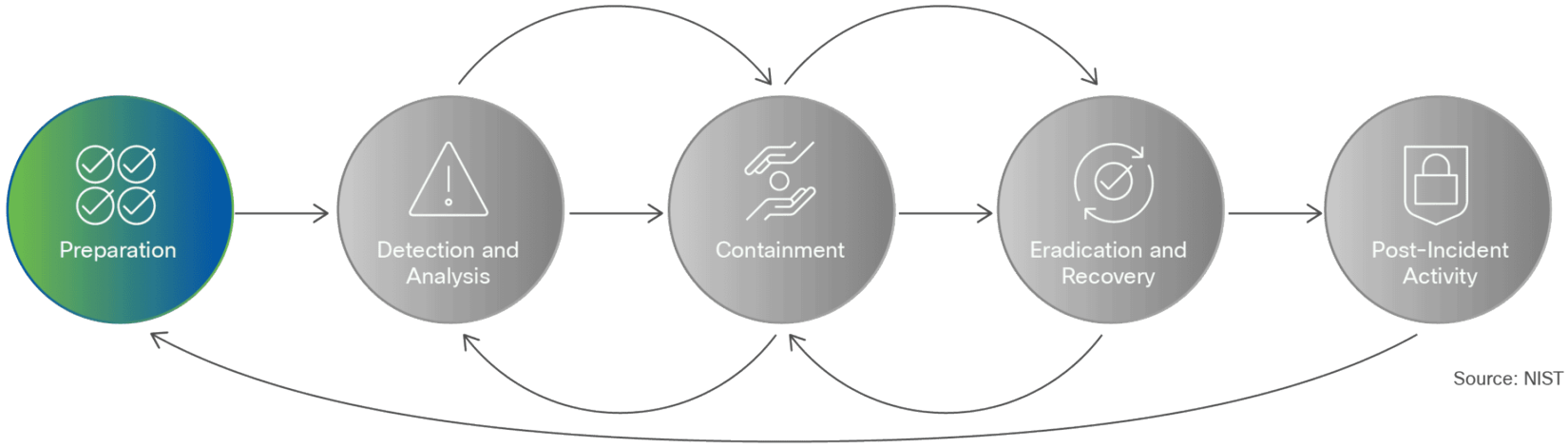
Use Case 1:

Preparation for security incidents

This is the cornerstone of your incident management protocol and probably the most essential stage in protecting your organization before an incident occurs. Organizations must have a predefined plan to address security incidents to help SOC teams deal with cyberattacks or data breaches. It is critical that SOC members are properly trained in their response roles and responsibilities in the event of a security incident.

In addition to documented processes and proper training, it is crucial for organizations to effectively prepare for a security incident by completing the following steps:

- Understand all protected surfaces, such as applications, endpoints, data, servers, communication infrastructure, etc.
- Identify all possible attack vectors potentially exposed to threats.
- Recognize the impact and implications if an attack is successfully perpetrated against protected assets.



Source: NIST

Cisco XDR, through Device Insights, provides increased visibility and management options to help organizations understand the surfaces that need to be protected.

Cisco XDR is designed to consolidate, discover, normalize, and work with your device inventory to identify all possible exposed attack vectors. Device Insights unifies multiple device managers, endpoint detection and response, AV, and other endpoint security products and then brings the details provided by those tools and solutions into a unified view to reduce the impact of an incident within your protected assets.

Cisco XDR improves your incident readiness, identifying gaps in control coverage so you can build custom policies and explore opportunities for playbook-driven automation.

As a part of this readiness program, NIST recommends the following:
"Exercises involving simulated incidents can also be very useful for preparing staff for incident handling."

NIST SP 800-84

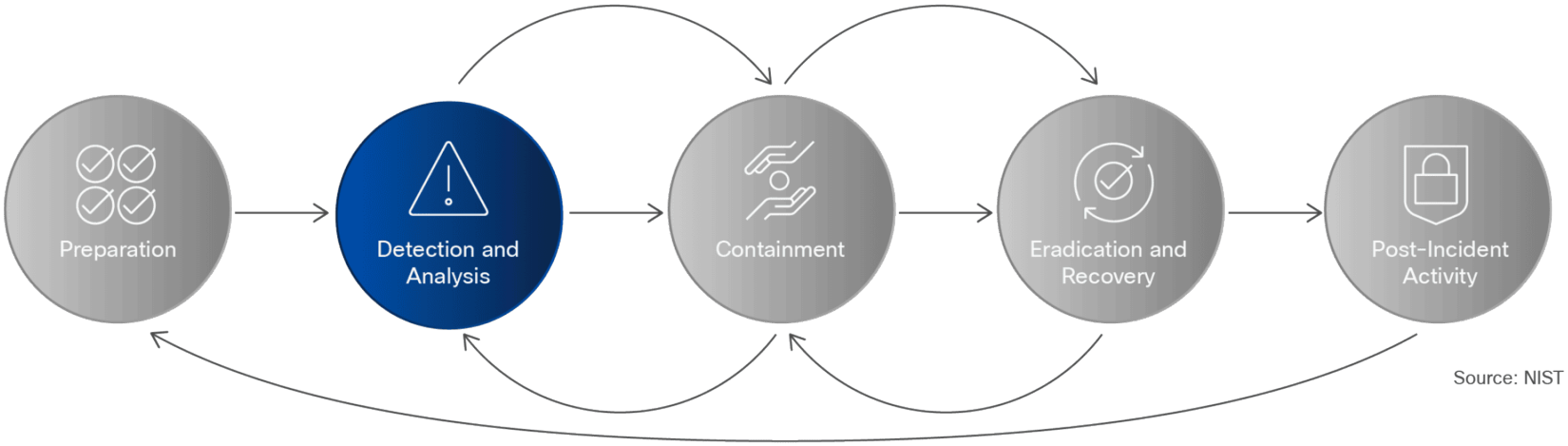
Use Case 2:

Threat detection and analysis

Security teams report that the most challenging stage of the security management cycle is detecting and assessing cybersecurity incidents.

Defining if an initial detection is declared as an incident is vital and, if so, the type, magnitude, and scale of the compromise within cloud environments, endpoints, applications, and network systems.

Dealing with sophisticated malware that can be extremely stealthy and capable of morphing from a benign to malicious state after crossing the point of entry is no easy task. Ransomware attacks have become increasingly prevalent and sophisticated, posing a significant threat to an organization's data and operations. These attacks can encrypt critical files, giving perpetrators leverage to demand a ransom for their release, causing severe disruptions and financial losses. Nefarious threat actors are widely leveraging different types of ransomware, like crypto ransomware, locker ransomware, scareware, leakware, and Ransomware as a Service (RaaS) to maximize their financial gains.



Source: NIST

As mentioned previously, threat detection is a foundational capability of any XDR solution, and it would be a starting point for further analysis efforts. It is not a matter of whether an advanced threat will strike, it is a matter of when. You must be able to accurately detect the threat so you can contain and neutralize it.

Keep in mind that novel techniques frequently leveraged by malware can make them extremely stealthy and capable of morphing from a benign to a malicious state after crossing the point of entry.

With continuous file analysis, Cisco XDR flags offending files such as mail attachments at the first sign of malicious behavior as indicated in the previous attack sequence. If a file is initially deemed safe, but after a few weeks begins to exhibit ransomware activity, Cisco XDR will detect the file and start the process of evaluation and analysis, while alerting your organization to act.

It is crucial for a SOC to have reliable and updated threat intelligence. Cisco Talos is a world-class threat research organization leveraged by Cisco XDR, providing expertise and resources to gather and analyze a wide range of threat data, including emerging threats and vulnerabilities. This ensures the SOC has access to the most up-to-date and comprehensive threat intelligence, allowing security teams to proactively gain valuable context and insights into the tactics, techniques, and procedures used by adversaries and threat groups.

Cisco XDR will automatically enrich these alerts using insights from multiple data

> **Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every possible incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies.**

NIST Computer Security Incident Handling Guide under section 3.2

sources and map the observed behaviors to the MITRE ATT&CK framework, so your security team can quickly prioritize and take immediate informed response actions to address threats based on their observed behavior and potential impact.

In summary, Cisco XDR utilizes adversary behavioral mappings combined with AI and ML threat detection capabilities to surface Zero-Day attacks at the entry point. Cisco XDR also supports advanced queries across all endpoints, email, cloud, and network security controls and continuously monitors all activity to detect stealthy malware and create high-fidelity alerts.

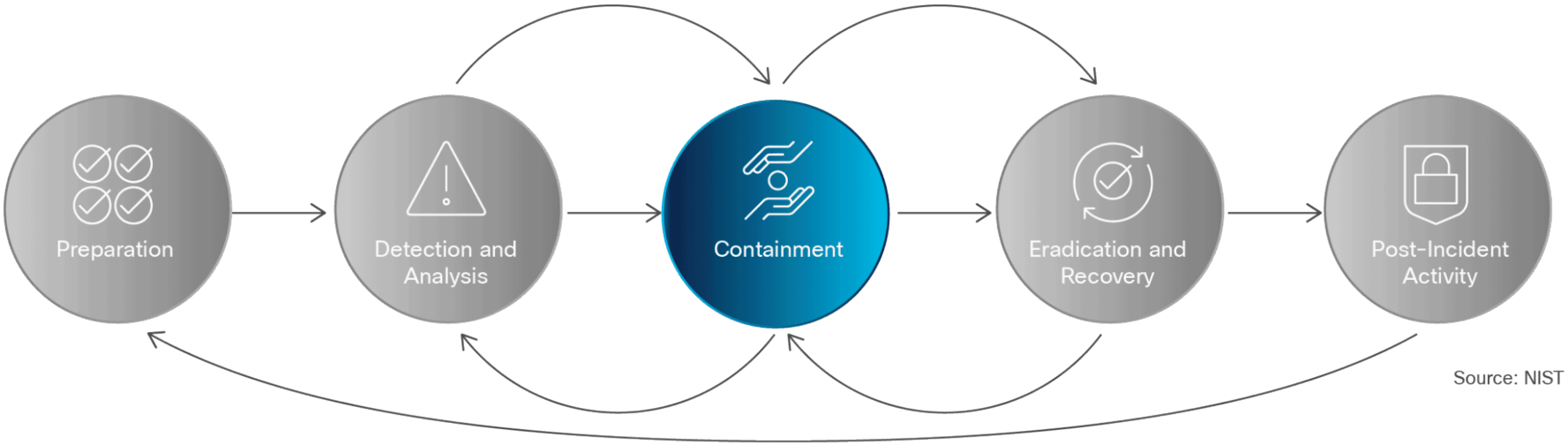
By implementing automated ransomware recovery powered by Cisco XDR in concert with third-party data backup solutions, organizations can minimize the impact of ransomware attacks. Automated recovery processes can swiftly identify and isolate infected systems, preventing the spread of ransomware throughout the network, while sending a request to the data backup solution to initiate a snapshot. This proactive approach helps to contain the attack and limit the damage inflicted.

Use Case 3:

Containment of a detected threat declared a security incident

Initial containment of a threat once it has been detected is a high priority step for a SOC team. This is especially vital during major incidents. Preventing further damage and reducing the immediate impact of a threat would be the main goals.

After detecting a malicious file in an attack scenario, Cisco XDR must be able to contain the threat. Malicious files aim to infect as many processes, applications, and users as possible. Micro-segmentation, as a part of our Cisco Zero-Trust strategy, can be a great defense within your data center to avoid lateral movement of advanced threats. While segmentation is helpful, a robust solution like Cisco XDR can help contain a malicious file before testing the edges of segmented areas of the network.



Source: NIST

Ransomware is a great example of why you need to contain threats at early stages to prevent the encryption of your information. In the next section when we cover the recovery stage of an incident management program, we discuss more details on how Cisco XDR assists with automated ransomware recovery capabilities.

As an additional control, Cisco XDR can isolate compromised endpoints, preventing further encryption over the network.

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

NIST

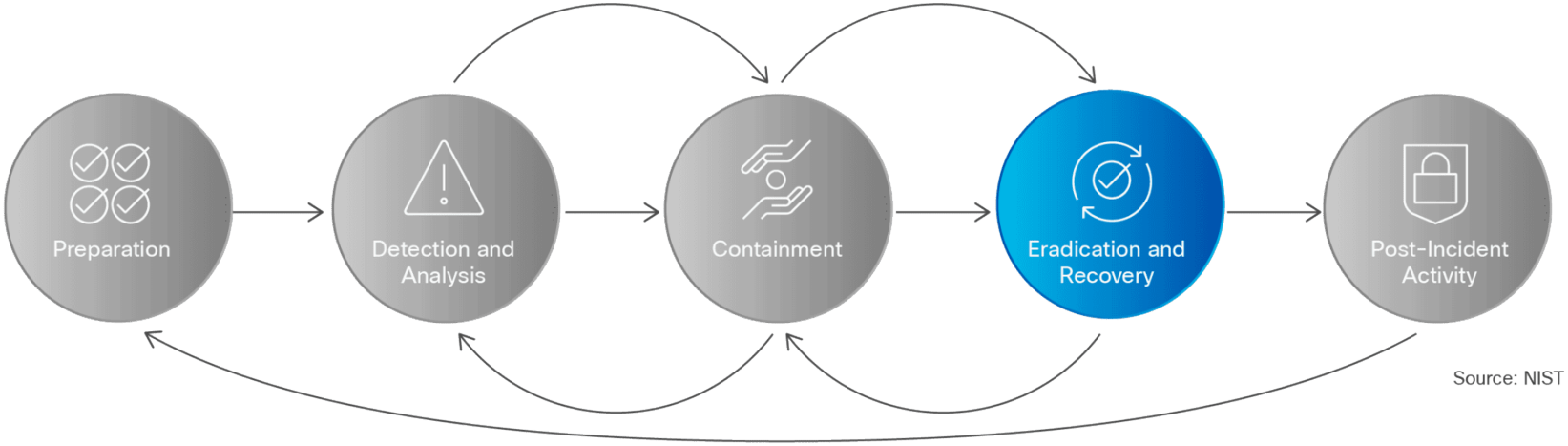
Use Case 4:

Eradication and recovery of an attack

At this stage of the incident management cycle, threat eradication followed by recovery tasks become top priorities for a security team. The goal of this phase is the return of normal operations by eliminating artifacts of the incident, such as removing malicious code, re-imagining infected systems, recovering network connections, and mitigating any exploited vulnerabilities.

Following our attack progression, once the malicious file has been detected and initially contained, an XDR solution should provide capabilities to investigate the incident. If the file snuck through the perimeter on the first try, there is a vulnerability. It's possible the threat intelligence team has never seen this kind of advanced threat before. Maybe a device or application needs to be updated.

Without proper investigative capabilities, your SOC team will not understand how a threat got through. As a result, your environment is likely to remain vulnerable to these same



Source: NIST

threats and issues again. Cisco XDR provides the type of per-incident review required to reveal these issues so your team can prevent future exploitation via the same threat vector.

Sandboxing is another critical capability in the investigative process. Sandboxing is when the file is isolated into a simulated environment, tested and monitored, and can be used at the perimeter to help grant or deny access, and can also be used just as effectively after the point of entry. Cisco XDR provides sandboxing through integrated Cisco Secure Malware Analytics.

Within this simulated isolated environment, Cisco XDR will try to determine the nature of the file without risking the safety of the larger environment. Through this process, Cisco XDR can understand the attributes and nature of this malicious file, then learn from it and adapt to better defend against future threats.

The most critical component of any XDR tool is its ability to eradicate the threat. Detecting, containing, and investigating a threat is a great start, but if you cannot eradicate it, your system remains compromised.

To properly eradicate threats, an XDR solution needs comprehensive visibility to answer questions such as:

- Where did the file originate?
- What different data and applications did this file interact with?
- Has the file replicated?

Visibility is crucial for eradication. Being able to see the entire timeline of a file is key. However, it's not as easy as simply removing the malicious file you have observed. When you eliminate the file, you likely may need to automatically remediate multiple parts of the network. For this reason, the Cisco XDR solution provides actionable data on the lifespan of the file. Cisco XDR has retrospective capabilities; this actionable data is used to automatically remediate systems to their state prior to infection.

Let's revisit the detection section of this document where we previously talked about the rise of ransomware strains that target organizations for financial gain. Unfortunately, recovering from a successful attack can be a time consuming process. With the increasing sophistication of these attacks, it's crucial for organizations to remain vigilant and proactive in their cybersecurity approach. Automated Ransomware Recovery with Cisco XDR enables organizations to detect the earliest signs of a ransomware outbreak by identifying the attack chains that precede the malware, so they can trigger a backup request which makes it easier to restore their systems to a pre-attack state efficiently. Traditional manual recovery methods can be time consuming and error prone, leading to prolonged downtimes and increased costs. Automation streamlines the recovery process, reducing the time required to recover critical data and minimizing operational disruptions. (See Automated Ransomware Recovery with Cisco XDR.)

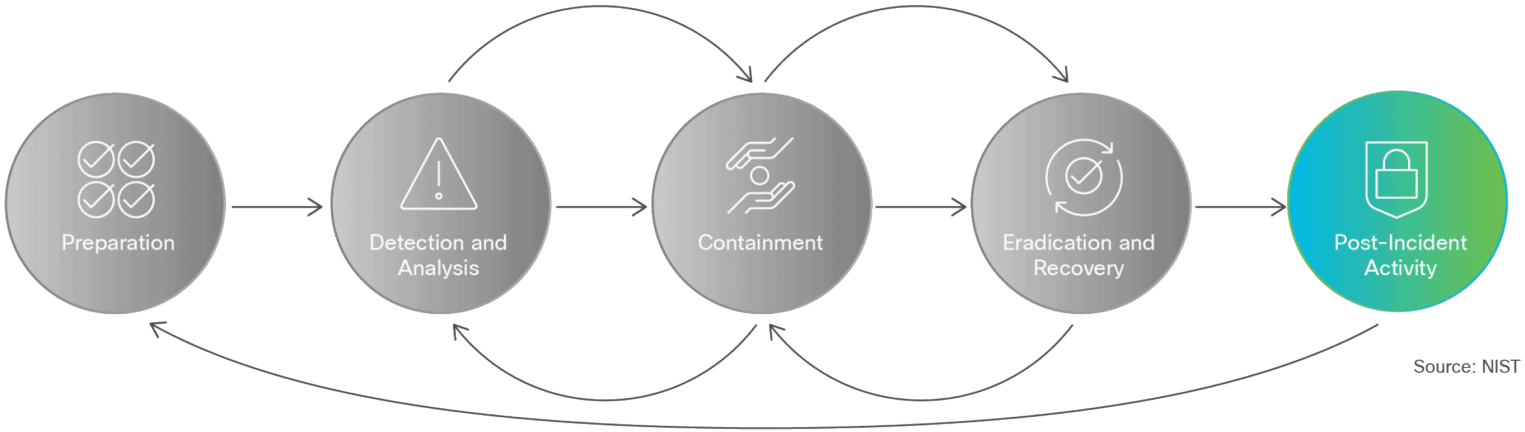
Use Case 5:

Post-incident analysis – lessons learned

At this last phase after the containment, eradication, and recovery stages, security teams examine the incident to gain understanding of how the it began. To put it simply, this stage is about getting to the root cause of how and why this incident occurred and, ultimately, elevating overall security posture. NIST Computer Security Incident Handling Guide under section 3.2.5 recommends that incidents should be immediately documented when the incident is declared so all facts are properly recorded.

Three top tasks that apply to any post-incident analysis process are:

- Document the incident and ensure the root cause has been eradicated or mitigated.
- Address vulnerabilities and infrastructure problems.
- Review and update roles, responsibilities, interfaces, and authority of security team members.



Source: NIST

An XDR solution needs to provide a comprehensive set of reports including all actions taken during each phase of the incident management cycle. Cisco XDR provides advanced capabilities such as detailed sample analysis reports, process execution charts, and direct user interaction with malware that can help security teams expose the root cause of an incident.

Cisco XDR also includes an advanced threat scoring system and behavioral indicators that are backed by advanced search capabilities across processes, file, disk, memory, network, and network artifacts and present findings to reinforce your preparation for future incidents.

Cisco XDR allows security teams to refine their security playbooks for future incident handling while permitting all roles within your SOC to quickly understand the details of an incident.

As it was covered in this document, Cisco XDR offers a unified XDR solution that helps across all stages of your SOC incident management program, enabling your security teams to block threats across multiple control planes and multiple vendor solutions more efficiently.

Cisco XDR and security resilience

Extended Detection and Response: a crucial component of security

By now, most organizations are used to operating under varying degrees of uncertainty. What sets truly resilient groups apart is their ability to address threats head-on and use those experiences to prepare for the future.

The right XDR tool puts your organization on the path toward security resilience. It will improve your security posture by empowering security teams to detect threats sooner, prioritize threats by impact, and accelerate response.

Why Cisco XDR?

If you're looking to simplify your security operations, look no further than Cisco XDR. By ingesting and correlating data and telemetry from a broad range of security solutions – (network, endpoint, email, identity, sandboxing, firewall, and more) Cisco XDR enables your SOC analysts to detect, investigate, and remediate threats in just a few clicks.

It's open, extensible, and cloud-first, so you can leverage your existing security investments and gain unified threat detection across your entire environment.

And XDR is just the beginning.

We want to partner with you on your security resilience journey, so Cisco XDR is powered by the Cisco Security Cloud – an open security platform aimed at helping you protect users, devices, and applications across your entire ecosystem, no matter what comes next.

Learn More

- Explore Cisco XDR
- Try the Cisco XDR self-guided demo
- Cisco XDR: Security Operations Simplified eBook
- XDR Buyer's Guide

Appendix A

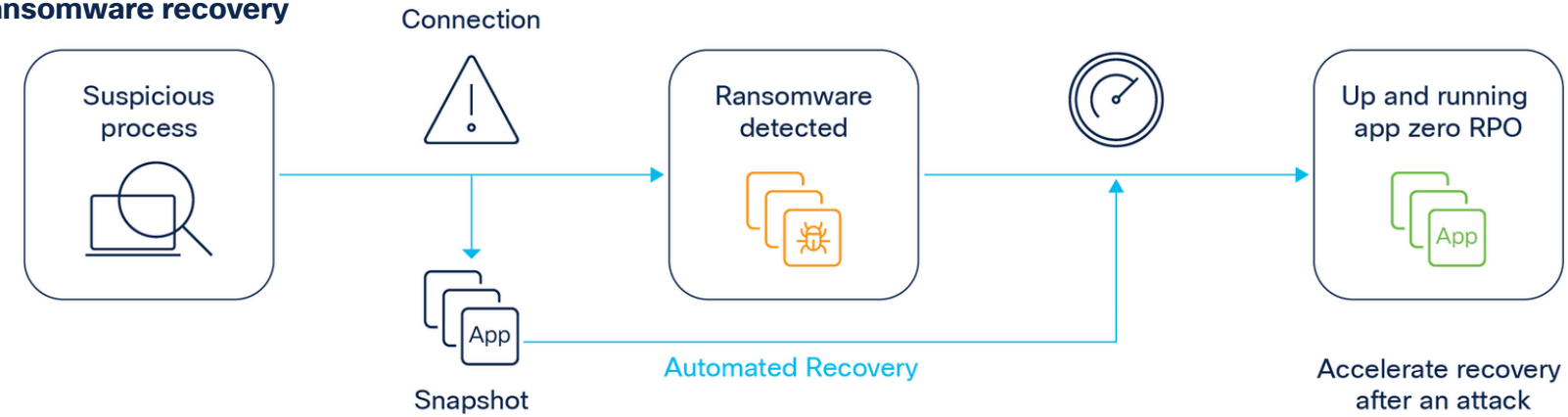
Automated Ransomware Recovery

Powered by Cisco XDR in partnership with leading enterprise backup and recovery vendors, Automated Ransomware Recovery reduces the risk of data loss during an attack by ensuring that the most important data is backed up more often when the ambient threat level is high. When the threat level recedes, backup policies are automatically relaxed.

This is how it works:
Ransomware attacks can tarnish an organization's brand image, erode customer trust, undermine organizational relationships, and threaten its viability and continued operations.

This is where the efficacy of Cisco XDR comes in by integrating with multiple security tools, even third-party solutions, already in place. This enables the SOC team to quickly identify the source of the attack leveraging cross-domain telemetry and take actions to stop the effects of ransomware.

Prevent data loss:
Automated ransomware recovery

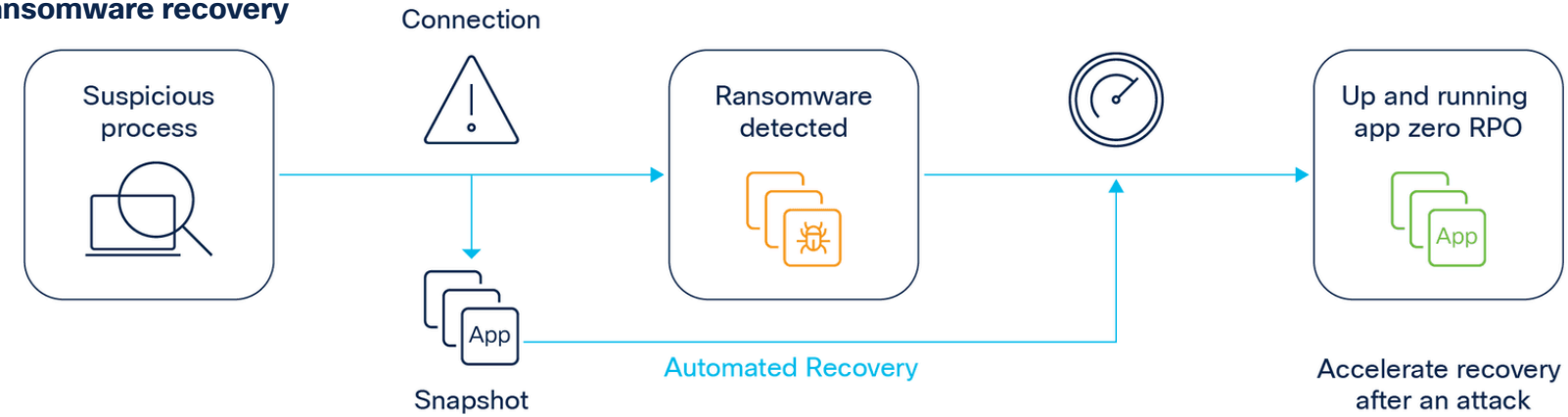


Respond instantly to protect critical data

Step 1:

In this scenario, a suspicious process is trying to establish a connection into an application that could be, as an example, a sensitive database. Cisco XDR can detect the ransomware attack attempt early and stop it leveraging insights from Cisco Talos and other third-party threat intelligence solutions for high accuracy, preventing the creation of false positives, and alerts the SOC as a part of the identification and containment stages for the incident management. However, let's assume that this is a targeted zero-day ransomware attack. In this case, a snapshot of the destination application is taken by a third-party data backup solution before the connection with unknown reputation is made. If the connection happens to be a ransomware attack, the snapshot is used to trigger an automated recovery request reducing the potential impact covering the recovery stage of the incident management program. If the connection is harmless then the snapshot is automatically discarded with no impact to operations.

Prevent data loss:
Automated ransomware recovery



Respond instantly to protect critical data

Step 2:

The security team can continue with the containment and eradication stages of the incident response program isolating the infected devices and preventing the malware from spreading further. Cisco XDR helps the security team to analyze the attacker's behavior, environment entry points, and techniques deployed.

Step 3:

The organization stopped and recovered from a novel ransomware attack. The SOC team uses Cisco XDR to implement additional security measures to prevent future attacks as a part of the Lessons Learned and Preparation stages of the incident management program.

While preventing ransomware is always the goal, when that isn't possible due to all evolving attacker techniques, swift and effective recovery measures are crucial to recovering and restoring full operational readiness. Security teams can now automatically detect, snapshot, and work with IT counterparts to restore business-critical data at the very first signs of a ransomware outbreak; often before it has had a chance to move laterally through the network to reach the high-value assets.

Thank you for reading

5 Ways to Experience XDR