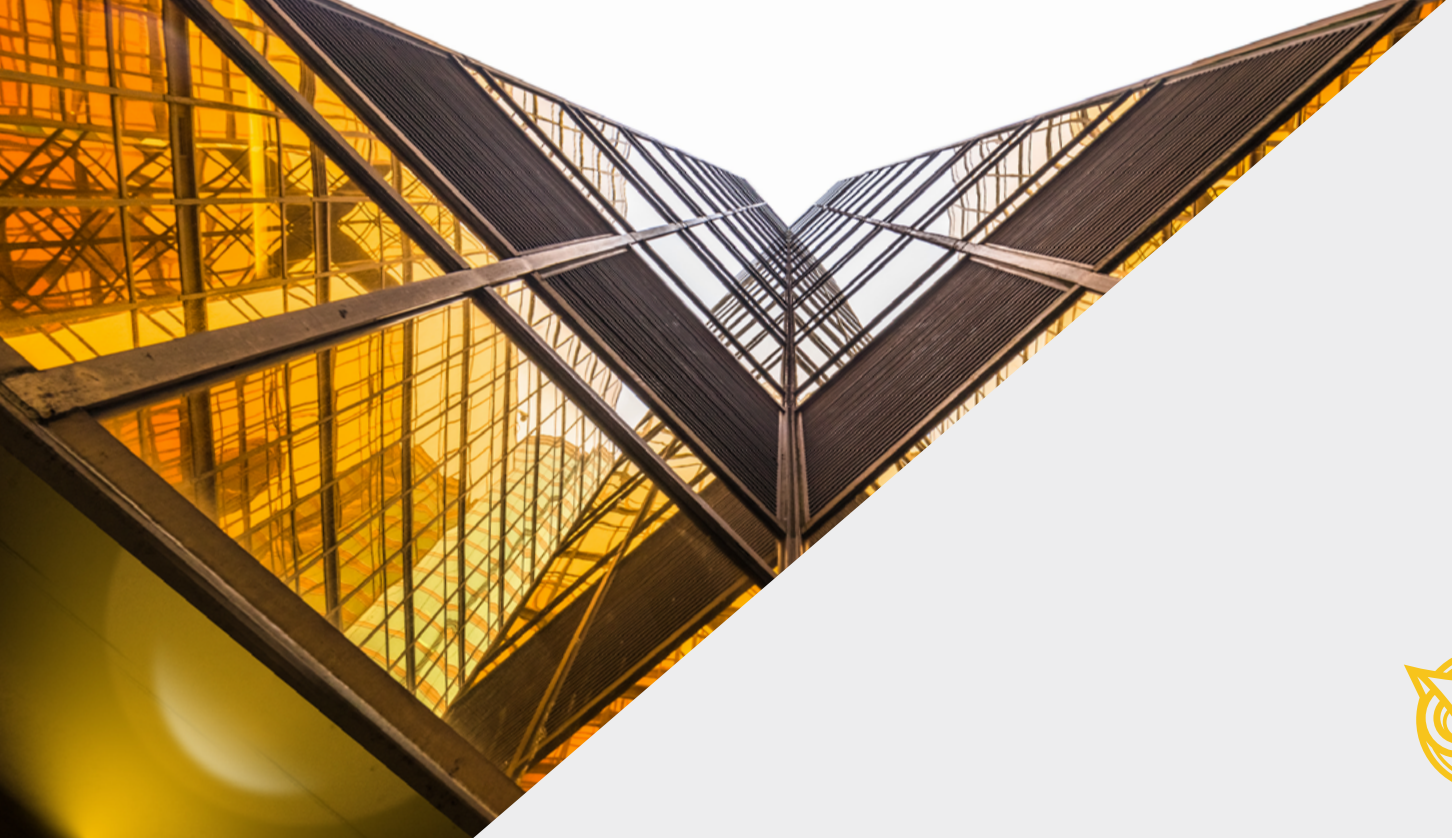
The Definitive Guide

TO ACHIEVING 10X THE SECURITY RESULTS WITHOUT 10X THE WORK

XDR®
POWERED BY GOOGLE CHRONICLE

cybereason®



Contents

XDR
POWERED BY GOOGLE CHRONICLE

Introduction

For the vast majority of security practitioners, the cyber threat landscape is spiraling out of control.

Increasingly sophisticated adversaries have gained a significant advantage over traditional approaches to threat detection and response, while defenders struggle with a skills shortage, lack of visibility into an ever-expanding attack surface, and too many siloed security tools that overwhelm analysts with alerts and false positives.

Today's siloed strategies are expensive and can introduce blind spots or result in ineffective coverage. In addition, investigating a broader malicious operation requires a complex workflow and staffing with domain expertise. To date, the overall result has been unacceptable response times measured in hours, days, weeks, or even months.

This is where the promise of eXtended Detection and Response (XDR) comes into play. The promise of XDR is to provide security analysts with better visibility into the attack surface, and the ability to take action quickly across multiple security layers. It is no longer enough to rely on Security Information and Event Management (SIEM) solutions that do little more than generate alerts and Security Orchestration, Automation and Response (SOAR) solutions that require an upfront investment in playbook development to respond primarily to known malicious activity. Cybereason XDR powered by Google Chronicle gives defenders a major advantage over the adversary. It is the only AI-driven XDR platform with the power to predict, understand, and end attacks at planetary scale.

XDR
POWERED BY GOOGLE CHRONICLE

Cybereason is capable of analyzing more than 23 trillion security-related events per week — five times the volume of any other solution in the market. Using its patented Malicious Operations (MalOps™) engine, Cybereason reveals the full attack story across every device, user identity, application, and cloud deployment. Meanwhile, Google Chronicle ingests, normalizes, and analyzes petabytes of data from the complete IT environment on planetary-scale infrastructure.

The combination of these capabilities delivers a cloud-native, AI-driven XDR solution that automates prevention for common attacks, significantly improves detection and incident response, and enables threat hunting with precision at a pace never before achieved.

Cybereason delivers a new benchmark for XDR that improves security operations by a factor of 10X. That means:

10X

- REDUCTION IN FALSE POSITIVES
- FASTER THREAT HUNTING AND INTELLIGENCE MANAGEMENT
- PRODUCTIVITY BOOST FROM UNIFIED INVESTIGATIONS
- FASTER RESPONSE TIMES, FROM HOURS TO MINUTES

This is Cybereason XDR - delivering 10x the results without 10x the work. What follows is an overview of how the industry's new benchmark in XDR platforms addresses the most pressing operational and business challenges facing cybersecurity leaders and teams.

XDR
POWERED BY GOOGLE CHRONICLE

10XDR

Solving Real Business & Operational Challenges at Scale

According to ESG research, enterprise organizations state that improving detection of advanced cyber-threats is their highest security operations priority. As a result, 83% of organizations will increase threat detection and response spending over the next 12 to 18 months.

But XDR can do more than simply improve detection and response. "Beyond threat detection and response, CISOs should think of XDR as a catalyst for modernizing the SOC, automating processes, and improving staff productivity," wrote ESG Senior Principal Analyst John Oltsik.

83%

of organizations will increase threat detection and response spending over the next 12 to 18 months.

XDR
POWERED BY GOOGLE CHRONICLE

10X REDUCTION IN FALSE POSITIVES

PROBLEM

Security Operations Center teams, regardless of size or sophistication, are at their breaking point. Alert overload and a "Fear of Missing Incidents" have led to unmanageable stress levels for SOC analysts. Making matters worse, more than half of those alerts are false positives — robbing analysts of time they could use on planning, training, and proactively improving their security program.

TODAY'S TOOLS ARE FAILING

SIEM tools, intrusion detection systems (IDS), email protection tools, and firewalls can be notoriously "noisy," firing off large volumes of alerts with limited context into the root cause, incident scope, and attack prioritization. It's up to the human analyst to make sense of the alerts, track down impacted users and assets, and determine if it's true malicious activity.

Alert-centric security approaches are slow, inefficient, and costly. One of the main challenges that most security teams face is dealing with too many alerts across numerous, siloed consoles. While nearly every detection technology available today maps to the MITRE ATT&CK framework, too many technologies simply "alert" on threats; they don't block malicious activity or enable faster, accurate incident response.

Over time, false positives desensitize your team to real threats. When facing massive volumes of false alerts, teams may change the threshold for alerts to be less sensitive or turn off protections entirely. Human processes simply cannot scale fast enough to handle the increasing volume of false positives and real threats.

THE PROMISE OF XDR

For the first time, Cybereason XDR links together the many ways we work: on remote endpoints, mobile devices, cloud services and email, and uses this data to expose a broader attack story. For example, if Bob's laptop blocks malware, or exhibits indicators of compromise, where did it originate — a spear-phishing email, cloud drive, or a USB key? And, is anything happening with Bob's broader identity across email, chat, cloud services, or assets that are a lateral hop away?

This is where AI must be used to both distinguish between benign and malicious behavior, and link behaviors across assets and identities for faster root cause analysis and incident scoping. With a focus on identifying a broader operation, instead of individual malicious behaviors, the role of human analysts is instantly elevated. Their role shifts away from chasing false positives to analyzing all possible attack sequences in the context of the business' operations, and taking the steps necessary to reduce the organization's risk and protect its reputation.

The most advanced AI-driven XDR solutions can predict the likely next steps in any given malicious operation, allowing defenders to proactively take remediation actions to reduce risk and achieve their mission of protecting crown jewels.

XDR
POWERED BY GOOGLE CHRONICLE

10X FASTER THREAT HUNTING AND INTELLIGENCE MANAGEMENT

PROBLEM

For many Security Operations Centers (SOCs), conducting useful queries using a traditional Security Information and Event Management (SIEM) requires training and familiarity with syntax language, and deep analysis to take action on the results of a particular hunt. At enterprise scale, searches can take several minutes or longer to complete, making it cumbersome to derive new insights or successfully connect threat intelligence and investigate matches. Threat intelligence is often only matched against newly ingested data, creating coverage gaps and missed threats.

TODAY'S TOOLS ARE FAILING

As an aggregation tool for logs and event data, SIEMs can support broad data sets but struggle to correlate and present meaningful insights around malicious behaviors.

As an example, few organizations look to feed endpoint telemetry into their SIEM because:

1. It's challenging to create nuanced detection rules.
2. Searches and queries struggle to perform at scale.
3. Data ingestion and retention aren't worth the high cost.

Therefore, most teams compromise by sending the alerts to the SIEM. But, SIEM isn't great at correlating disparate events across email, identity, endpoint, network, and cloud in an actionable way. Often, to compensate for the high cost of SIEM data storage needs, a good deal of event data is filtered out, thereby further diminishing the effectiveness of the SIEM investment.

Traditional endpoint security solutions also limit or filter some of your valuable data because they simply cannot handle processing and storing it, which gives you reduced visibility and makes it impossible to actually leverage your data. Your XDR solution must ensure all of your relevant data is collected, processed, and analyzed in real-time, and, if you choose, accessible indefinitely.

THE PROMISE OF XDR

Cybereason XDR leverages a new security paradigm that uses artificial intelligence to correlate the behaviors that take place across the many ways we work: on endpoints, across identities, and on public and private networks, including protecting IoT devices and cloud infrastructure.

Cybereason XDR takes the Indicators of Behavior (IOB) concept from EDR but widens the scope to the modern distributed IT environment. This includes integrations with email, productivity suites (e.g. Microsoft & Google), network data, and cloud infrastructure.

Cybereason XDR enables comprehensive monitoring across the entire attack surface to identify patterns and detect potential threats on a broader scale—connecting the dots between seemingly disparate or innocuous events to recognize indicators or behavior and take action to prevent or stop threats.

At a minimum, expect the XDR solution to have a cloud-native data storage strategy, the ability to scale as your enterprise and data ingest grows, and a threat detection strategy validated by leading technical testing, such as the MITRE ATT&CK APT Evaluations.

XDR
POWERED BY GOOGLE CHRONICLE

10X PRODUCTIVITY BOOST FROM UNIFIED INVESTIGATIONS

PROBLEM

Manual analysis of logs can be a time-consuming process. Today's siloed strategies are expensive and often lead to blind spots or ineffective coverage. Investigating a broader malicious operation requires labor-intensive workflows and multiple analysts with diverse domains of expertise.

TODAY'S TOOLS ARE FAILING

Much of the interest around XDR stems from a demand for actionable incident response against top threats like ransomware, business email compromise, and account takeover.

Most systems are collectors of security and related telemetry, with only the occasional behavior revealed in the process. What's needed is more behavioral instrumentation of the available telemetry to create the capability to recognize chains of behavior that may be malicious. Defenders are also struggling with Endpoint Detection and Response (EDR) platforms that rely on more and more integrations, without the ability to correlate malicious behaviors across multiple assets. Increasing data in this way leads to alert fatigue, increases the chance of human error, and slows response times.

In addition, defenders desperately need response automation and guidance so they can quickly and accurately end a malicious operation.

THE PROMISE OF XDR

Cybereason XDR provides security teams with a multi-layer response framework, ranging from automatic prevention of threats like ransomware to guided response on what to do for each part of a detected malicious operation. This includes the ability to directly take response actions across endpoints, identities, and networks.

XDR delivers enhanced correlations across IOCs and IOBs

Cybereason XDR delivers enhanced correlations across Indicators of Compromise (IOCs) and key Indicators of Behavior (IOBs), the more subtle signs of network compromise. Unlike SIEM and UEBA correlations, being able to visualize the entire story of an attack produces a much higher true-positive rate and augments the intuitions of your SOC team.

This operation-centric approach also enables defenders to share high-fidelity detections with other defenders that are effective in any environment with any combination of hardware and software. This arms the larger community of defenders worldwide to collectively create a unified front to confront the attackers where they operate, in real-time and at scale, and usher in an age of democratized security where organizations are no longer at risk due to a lack of resources or capabilities.

XDR
POWERED BY GOOGLE CHRONICLE

10X FASTER RESPONSE TIMES, FROM HOURS TO MINUTES

PROBLEM

Despite spending millions of dollars on cybersecurity tools over the past few years, most organizations still can't detect or respond to cyber attacks in a reasonable timeframe. According to Verizon's 2021 Data Breach Investigations Report (DBIR), 60% of incidents were discovered within days. However, in 20% of attacks, it took months or longer before organizations realized a breach had occurred.

TODAY'S TOOLS ARE FAILING

In most cases, an organization's response time to a cybersecurity incident is a function of the quality of the alerts produced by the security tools deployed. The higher the quality and context of the initial alert, the faster the team can investigate and respond.

To date, monitoring technologies have produced low-quality alert signals that lack supporting context. The problem has been compounded by the fact that most organizations have tried to overcome this challenge by adding more security tools to their tech stack. The results have been predictable: out-of-control tool sprawl and continuous integration complexities.

THE PROMISE OF XDR

Cybereason XDR breaks down traditional data silos that attackers use to remain undetected by unifying device and identity correlations for faster, more effective threat detection and response. Advanced solutions add predictive analytics to enable defenders to anticipate an attacker's next steps and proactively mitigate risk.

> The key to effective incident response is an operation-centric approach.

Unlike SIEM, Cybereason XDR comes with native response capabilities that eliminate having to work with IT to take incident response action. Guided and automated response capabilities further empower analysts and reduce errors. In many cases, organizations should consider partnering with a Managed Detection and Response provider that can take actions using the Cybereason XDR console and is backed by swift response service-level objectives (SLOs).

The key to effective incident response is an operation-centric approach. Each incident has a root cause, a range of affected users and assets, a timeline of activity, and a level of severity -- what will happen if no action is taken?

Cybereason XDR moves an organization's security posture from simply automating repetitive security tasks to a state of "detect, understand, and anticipate." With direct access to meaningful security data across your environment, Cybereason XDR can predict areas of future risk and suggest actions to take to get ahead of your most probable security threats.

XDR
POWERED BY GOOGLE CHRONICLE

POWERED BY GOOGLE CHRONICLE

Cybereason XDR

Cybereason and Google Cloud have formed a strategic partnership to bring to market a joint solution in support of our mission to reverse the adversary advantage. This pivotal partnership has placed artificial intelligence (AI) at the center of XDR to create the world's most powerful cyber defense solution.

Cybereason XDR Powered by Google Chronicle can easily ingest and analyze petabyte-scale telemetry across the complete IT and security stack and offers unrivaled speed and accuracy for the prevention of advanced threats against endpoints, networks, containers, application suites, user personas, and cloud infrastructure.

XDR
POWERED BY GOOGLE CHRONICLE

The Cybereason and Google Cloud partnership creates the most powerful unified AI-driven XDR solution available on the market today that delivers protection, response, and attack prediction across the modern IT and security stack. Cybereason XDR Powered by Google Chronicle leapfrogs first-generation XDR solutions and makes the promise of AI-driven XDR a reality: the ability to predict, detect and respond to cyberattacks at infinite scale and maximum speed.

AI-driven XDR from Cybereason is the only XDR platform capable of gathering telemetry across the planetary attack surface and delivering 10X performance improvements for defenders.

AI-driven XDR from Cybereason breaks down the data silos that attackers rely on to remain undetected by unifying device and identity correlations for 10X faster and 10X more effective threat detection and response while unlocking new powers of prediction that enable defenders to anticipate and end future attacks before they begin.

This cutting-edge innovation leapfrogs first-generation XDR solutions and makes the promise of artificially intelligent XDR a reality to deliver:

PLANETARY-SCALE PROTECTION

AI-driven XDR from Cybereason combines the Cybereason MalOp, which analyzes over 23 trillion security events per week to deliver instant detection and incident response, with Google Chronicle's unrivaled ability to ingest and normalize petabytes of data from the entire IT environment for planetary-scale protection.

OPERATION-CENTRIC DETECTION AND RESPONSE

Instead of being alerted about individual events, users can instantly understand the entire attack progression across every device, user identity, application and cloud deployment to end them immediately. The Cybereason MalOp provides automated and guided response actions to reduce human error, upskill analysts, and achieve a 10x faster time to response than competing solutions.

PREDICT ATTACKER BEHAVIOR

Defenders can shift from a labor-intensive, alert-centric posture to a predictive operation-centric model. Through context-rich correlations, AI-driven XDR from Cybereason identifies subtle signs of malicious behavior and predicts an attacker's likely next steps to anticipate and proactively block attacks.