CISO GLOBAL

Example Use Cases

XDR REAL WORLD APPLICATIONS

As with any relatively new technology, you may have found yourself wondering about XDR, “What can it do for me and my organization?” These five real-world applications of XDR illustrate its capabilities.

XDR IN THE REAL WORLD

CASE 1

Combined Services in a Single Offering

The Challenge

Vendor sprawl increases workload for security teams, driving up costs, MTD and MTR. Different vendors represent data in different ways, with no inter-vendor correlation. With multiple security platforms protecting the environment, analysts must constantly switch between them, trying to make sense of disparate data sets to understand and respond to security events.

The XDR Solution

XDR provides a correlation platform allowing you to see all your security events in a single pane of glass and a common format. A single provider also facilitates simpler management by your teams of your existing technology.

The Result

By supporting, correlating and analyzing all telemetry, XDR enables clear understanding and swift, effective security decision-making, avoiding data incongruence and portal overload, and reducing vendor management costs.

CASE 2

Cloud Architecture Security Alert Monitoring

The Challenge

Cloud infrastructure alerts from platforms such as Google Suite, Amazon AWS, Microsoft Office 365 and Azure often sit in silos. Flagging events such as suspicious logins and brute force activity, they are typically sent to the account administrator. However, with in-house professionals often stretched thin, around-the-clock oversight of such alerts may be unrealistic. This is problematic, as alerts can indicate wider attack trends, as well as identifying issues within the specific cloud platforms related to each alert.

The XDR Solution

XDR pulls all telemetry into the SOC, where alerts are correlated and triaged. In superior XDR solutions, this is undertaken automatically, using automated playbooks that are fully customized according to the organization's needs. Cases are then passed immediately to experienced, certified analysts, giving them the necessary insight to accurately evaluate any actions required and perform more effective threat hunting across the organization's estate.

The Result

Cloud adoption is growing all the time, and as it does so, there is more information available for telemetry. XDR ensures this information is used beneficially for security decision-making rather than sitting in a silo, its value reduced or even lost. Failure to capture and leverage cloud information is one reason why business email compromise, for example, is an effective type of attack.

XDR IN THE REAL WORLD

CASE 3

Behavioral Analysis

The Challenge

Increasingly, cyberattacks employ approved account credentials and known good tools, avoiding the need for suspicious logins and malware, in order to remain covert within the organization's systems. Such attacks are substantially harder to detect than their predecessors.

The XDR Solution

To detect such attacks, XDR employs behavioral analysis to build a clear picture of typical behaviors of each server and each user on each day – we call this baselining. It then monitors actual behaviors, looking for divergence from the norm. When anomalous behaviors are detected, a certified analyst is notified, triggering immediate investigation. Covert attacks are identified, and stopped swiftly.

Many solutions, while baselining user behaviors (login times, assets used and login locations, for example) fail to do so for server behaviors, such as traffic patterns, inbound and outbound communications, and applications utilized. Unexpected user behavior will be flagged, but, for example, the quiet background transfer of data to a previously unknown IP address might not.

Superior XDR solutions leverage ML to undertake both network traffic analysis and end user behavioral analysis. Both are essential to build a complete picture.

The Result

With the benefit of enhanced security analyst responses, XDR enables the early detection and neutralization of covert attacks, even those employing only existing authorized user's credentials and known good tools.

XDR IN THE REAL WORLD

CASE 4

Automated Endpoint Remediation and Response

The Challenge

While the prompt detection of malicious activity is key to endpoint protection, it doesn’t go far enough. Immediate triage and remediation are essential to the protection of operational uptime and the swift restoration of order after a cyberattack.

The XDR Solution

Many endpoint events can be handled immediately and automatically by XDR, killing, quarantining and sandboxing rogue processes, undertaking remediation, and rolling affected endpoints back to a known good state.

The Result

With rollback as well as remediation, attacks are essentially reversed, protecting uptime and productivity on all protected endpoints. Such automation frees IT staff to focus on more serious security events, and accelerates the overall process in a layered attack.

XDR IN THE REAL WORLD

CASE 5

Around-the-Clock Security Monitoring

The Challenge

The majority of attacks are launched outside of office hours, at night or on the weekend. With traditional security solutions, lacking 24/7/365 monitoring, it is often impossible to identify and remediate attacks early enough to avoid significant damage.

The XDR Solution

Superior XDR solutions, built around SOCs operating with certified analysts 24 hours a day, every day, including holidays, can detect and address cyberattacks whenever they may be mounted.

The Result

Customers protected by such XDR solutions can enjoy their evenings, weekends and holidays confident in the knowledge that their systems are safe, that no bad actors have been inside the organization's accounts wreaking havoc in their absence. Intelligent software, monitoring telemetry from across their IT estate, and working hand-in-hand with certified cybersecurity experts, delivers improved threat hunting, identifying and neutralizing attacks earlier.

ABOUT CISO GLOBAL

About Us

CISO Global (NASDAQCM: CISO), based in Scottsdale, Arizona, is a Top #25 managed cybersecurity and compliance services provider and industry leader in proprietary software that is delivering innovative solutions through its newly developed AI and ML-powered product portfolio. The company protects the most demanding businesses and government organizations against continuing and emerging security threats and ensures their compliance obligations are being met. For more information about the company, visit CISO Global on LinkedIn, X or at www.ciso.inc.

RISK & COMPLIANCE

- Gap Analysis
- Audit & Assessment
- Third-Party Risk Management
- FedRAMP & StateRAMP
- Compliance Support
- Risk Advisory Services
- Virtual CISO
- Managed GRC
- TiGRIS
- 25+ Security Frameworks Supported

SECURITY OPERATIONS & INCIDENT RESPONSE

- Extended Detection & Response
- Managed Detection & Response
- Security Information & Event Management
- SOC as a Service
- Vulnerability Management Program
- Attack Surface Reduction
- Incident Response
- Digital Forensics
- Threat Intelligence

SECURITY ARCHITECTURE & ENGINEERING

- Cloud Security
- Data Protection
- Remediation
- Secure Network Architecture
- Identity & Access Management
- Secured Managed Services

SECURITY TESTING & CERTIFICATION TRAINING

- Penetration Testing
- Tabletop Exercises
- Training Programs
  -Security Testing Methodolgy
  -CMMC & Other Certifications
  -Security Awareness Training
- Red Team
- Purple Team
- Cloud, Network, Application, & Physical Pen Tests

AICPA SOC
SOC 2® Type II Audited

CISO
GLOBAL

480-389-3444 | ciso.inc