EXIUM

CATEGORY: Security Operations

Autonomous XDR for Unparalleled Security Operations Productivity

Solution: Extended Detection and Response ▪ **Industry**: Any vertical ▪ **Use Case**: Enhancing Security Operations Productivity

Exium's XDR can help you supercharge detection and response across your security stack giving security professionals the information and tools they need to respond to, contain and remediate sophisticated attacks — faster and more efficiently.

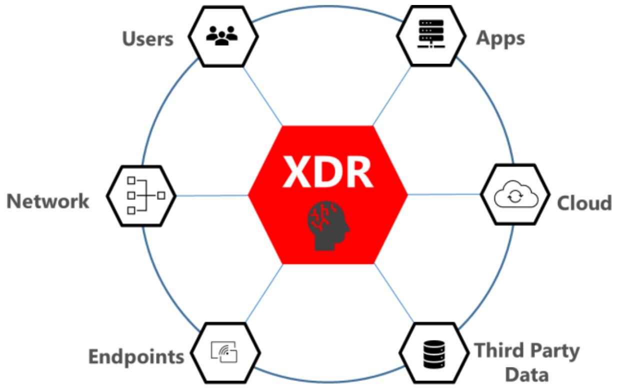
What Is Extended Detection and Response (XDR)?

Extended detection and response (XDR) capabilities provide visibility and actionable insights across networks, clouds, endpoints, and applications to help Security Operation Center (SOC) teams to hunt, investigate, and remediate threats.

XDR is an alternative to traditional approaches that provide only siloed visibility into attacks, such as endpoint detection and response (EDR), network traffic analysis (NTA), and security information and event management (SIEM). The problems with these reactive approaches are too many alerts that are incomplete and lack context and time-consuming, complex investigations that require specialized expertise. The result of these challenges is that threats go undetected for too long, increasing response time and raising the risk and consequences of an attack.

XDR vs. EDR

XDR represents the evolution of detection and response beyond the current point-solution, single-vector approach.



Clearly, endpoint detection and response (EDR) has been enormously valuable. However, despite the depth of its capability, EDR is restricted because it can only detect and respond to threats inside managed endpoints. This limits the scope of threats that can be detected as well as the view of who and what is affected. These restrictions ultimately limit response effectiveness within the SOC.

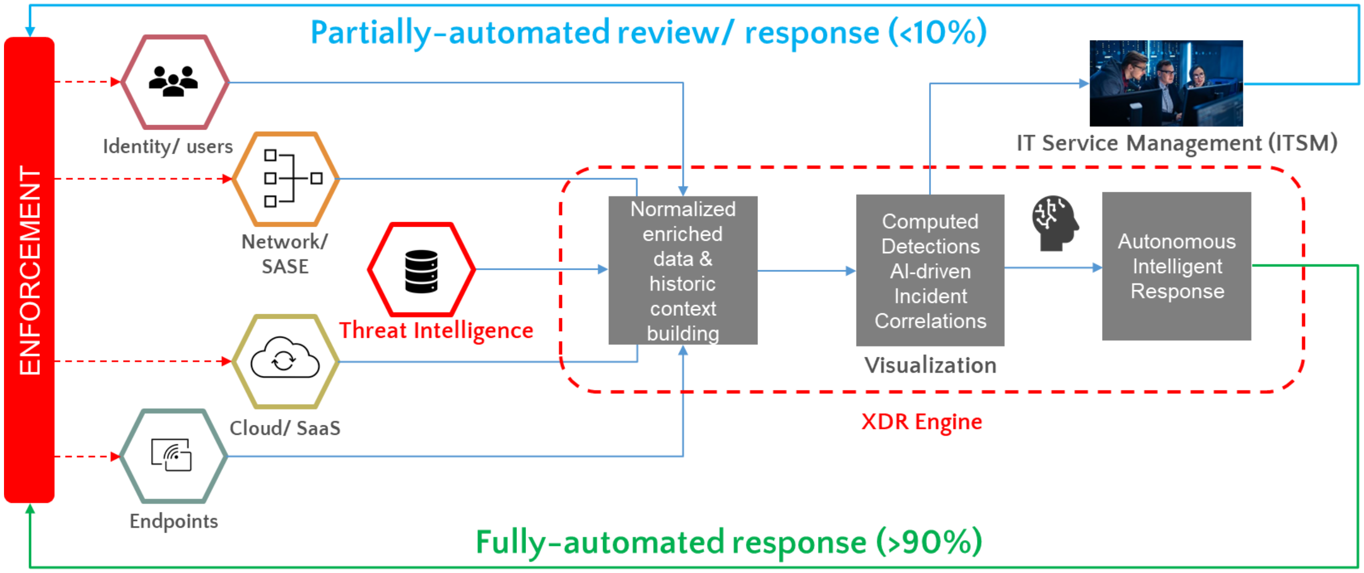
Likewise, network traffic analysis (NTA) tools' purview is limited to the network and monitored network segments. NTA solutions tend to drive a massive number of logs. The correlation between network alerts and other activity data is critical to make sense and drive value from network alerts.

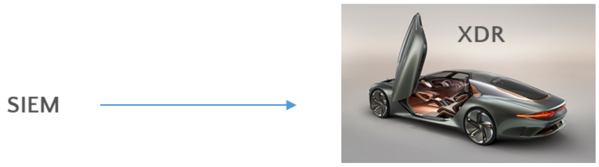
XDR vs. SIEM

Organizations use SIEMs to collect logs and alerts from multiple solutions. While SIEMs allow companies to bring together a lot of information from multiple places for centralized visibility, they result in an overwhelming number of individual alerts. Those alerts are difficult to sort through and understand what is critical and needs attention. Correlating and connecting all of the information logs to gain a view of the larger context is challenging with just a SIEM solution.

Conversely, XDR collects deep activity data and feeds that information into a data lake for extended sweeping, hunting, and investigation across security layers. Applying AI and expert analytics to the rich data set enables fewer, context-rich alerts – reducing the time required by security analysts to assess relevant alerts and logs and decide what needs attention and warrants deeper investigations.

XDR makes real-time threat detection easier by bringing together world-class threat hunting, machine learning (ML), artificial intelligence (AI) and threat intelligence with third-party data sources. Unlike SIEM, XDR delivers impactful remediation strategies by intelligently consolidating all of the valuable telemetry from security solutions, while also orchestrating and automating analysis.


Partially-automated review/ response (<10%)
ENFORCEMENT
Identity/ users
Network/ SASE
Threat Intelligence
Cloud/ SaaS
Endpoints
IT Service Management (ITSM)
Normalized enriched data & historic context building
Computed Detections AI-driven Incident Correlations
Visualization
Autonomous Intelligent Response
XDR Engine
Fully-automated response (>90%)



How does XDR work?

XDR connects data from siloed security solutions so they can work together to improve threat visibility and reduce the length of time required to identify and respond to an attack. XDR enables advanced forensic investigation and threat hunting capabilities across multiple domains from a single console.

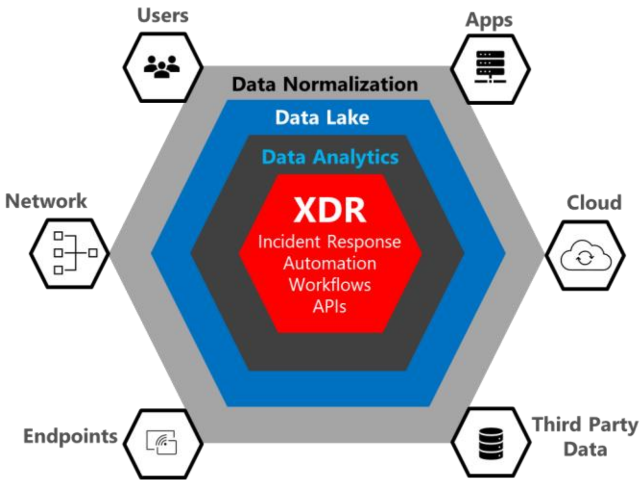
Here's a simple step-by-step of how XDR works:

Step 1. Ingest: Ingest and normalize volumes of data from endpoints, cloud workloads, identity, email, network traffic, virtual containers and more.

Step 2. Detect: Parse and correlate data to automatically detect stealthy threats with advanced artificial intelligence (AI) and machine learning (ML).

Step 3. Respond: Prioritize threat data by severity so that threat hunters can quickly analyze and triage new events, and automate investigation and response activities.

Step 4. Remediate: Unless a threat is simple, like commodity malware that can be easily cleaned up, remediation is typically delayed until a manual investigation is performed. XDR, on the other hand, provides security analysts both the visibility and ability to not just respond but also remediate. Security analysts and operators can take precise rather than broad actions, and not just across the network, but also the endpoints, apps, cloud and other areas.



Why XDR?

Many security products provide visibility into activity. Each solution offers a specific perspective and collects and provides data as relevant and useful for that function. Integration between security solutions can enable data exchange and consolidation. The value is often limited by the type and depth of the data collected and the level of correlated analysis possible. This means there are gaps in what an analyst can see and do. XDR, by contrast, collects and provides access to a full data lake of activity across individual security tools, including detections, telemetry, metadata, and netflow. Applying sophisticated analytics and threat intelligence, XDR provides the full context needed for an attack-centric view of an entire chain of events across security layers.

> *Not only did Exium XDR reduce the number of incidents we have to look at, but the time taken to act on those incidents was also reduced thanks to out of the box integration with our IT service management system."*
>
> **Director of IT Security Architecture, Global 2000**

XDR is a major step forward in enterprise security capabilities. Since XDR has access to raw data collected across the environment, it can detect bad actors that are using legitimate software to gain access to the system (something security information and event management software, or SIEMs, are often unable to do). It performs automated analysis and correlation of activity data, allowing security teams to contain threats more effectively.

Another important benefit of XDR is that it provides security teams the ability to investigate and respond to incidents from the same security technology platform. For example, an alert or analytics indicator might be generated from the endpoint which initiates an investigative workflow that is then augmented with network logs or other system logs that are part of the XDR platform for greater context. Instead of moving between different consoles, all the data sources are in one place. XDR enables security teams to resolve and close out a workflow on the same technology platform where it was initiated.

Key Features to look for in an XDR Platform

At its core, an XDR solution delivered from a cloud-native platform will dramatically improve threat visibility and reduce the length of time required to identify and respond to an attack. However, not all solutions are created equal.

Security teams should carefully consider which platform will serve as the foundation of their XDR functionality so that they can ensure comprehensive coverage, flexibility for the future and optimization of resources. Here we review some key questions organizations can ask when evaluating XDR vendors and their offerings.

> “
>
> *Exium’s XDR natively integrates the endpoint, network, cloud and user attack prevention & detection with the automated investigation and remediation capabilities, backed by a 24x7x365 world-class Managed XDR service.”*

Data

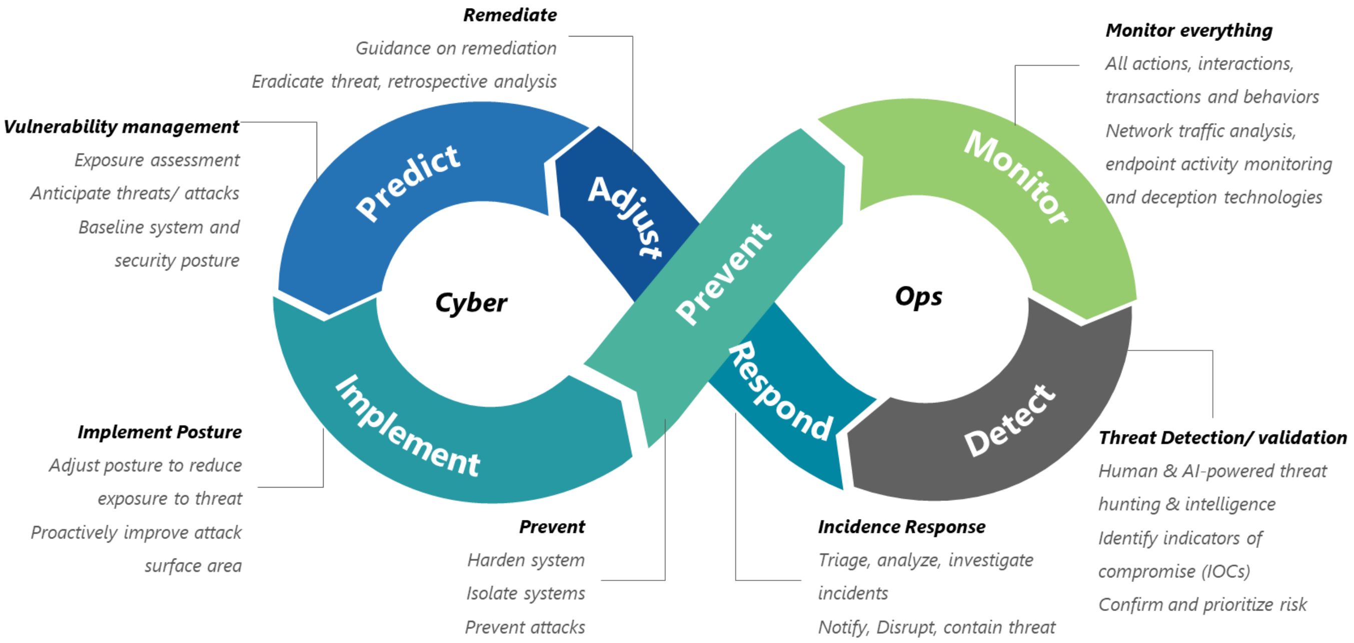
- ✓ Does the solution ingest and centralize data from security solutions across the enterprise?
- ✓ Does the solution leverage advanced automation and technologies such as artificial intelligence (AI) and machine learning (ML) to parse data, correlate it to the attack surface that was penetrated, and perform analysis and prioritization?
- ✓ Does the solution normalize the data, reorganizing it so that users can properly utilize it for further queries and analysis in threat hunting and investigation?
- ✓ Does the solution present security teams with this data in a single console that not only allows users to access cross-domain information for hunting and investigation but also to direct and orchestrate response?

Platform

- ✓ Is the solution vendor agnostic? Can it support integration with different tools, from different vendors?
- ✓ Are there any platform limitations that could impact the organization’s ability to integrate solutions in the future?
- ✓ Does the platform support advanced configurations and customization – including custom detections – based on the unique needs of each customer?
- ✓ Does the platform leverage open, well-defined schemas for data exchanges with additional IT security systems to ensure effective communication between security tools?

User experience

- ✓ Does the solution provide an intuitive and engaging user experience?
- ✓ What resources does the organization offer to help onboard new team members and ensure adoption and proper use?
- ✓ Does the provider support integrated security services (Managed XDR)?



Remediate

Guidance on remediation

Eradicate threat, retrospective analysis

Vulnerability management

Exposure assessment

Anticipate threats/ attacks

Baseline system and security posture

Monitor everything

All actions, interactions, transactions and behaviors

Network traffic analysis, endpoint activity monitoring and deception technologies

Implement Posture

Adjust posture to reduce exposure to threat

Proactively improve attack surface area

Prevent

Harden system

Isolate systems

Prevent attacks

Incidence Response

Triage, analyze, investigate incidents

Notify, Disrupt, contain threat

Threat Detection/ validation

Human & AI-powered threat hunting & intelligence

Identify indicators of compromise (IOCs)

Confirm and prioritize risk

CybeROC: 24x7x365 Managed XDR Team

Exium complements its autonomous breach protection technology with integrated security services at no additional cost. CybeROC is a 24/7 team of threat analysts and security researchers that leverage their expertise and Exium's vast threat intelligence feeds to provide various services to Exium's customers, in respect to each customer's specific needs and security preferences.

Alert Monitoring

The CybeROC team continuously monitors your environment – every hour of every day throughout the year. The team manages events, alerts, customer inquiries, and incidents.

The CybeROC team will proactively contact you when certain alerts or events are detected along with specific actions that should be taken.

Threat Hunting

CybeROC continually searches for new emerging threats in order to implement Indicators of Compromise (IoCs) and patterns into Exium XDR mechanisms. These proactive actions enable Exium XDR to collect, analyze, and alert for events while giving the forensics feature its ability to assess an entity's risk level.

Remote Incident Response

The CybeROC IR experts work in close partnership with the affected company to resolve incidents as fast as possible. Their process includes creating customized policies within the Exium XDR platform to scope and analyze the threat as well as providing recommendations and mitigations on the endpoint and across the IT and security environment.

Attack Reports

The CybeROC teams generates comprehensive reports in response to client questions. These Threat Research Reports contains an executive level summary, analysis description including involved processes, and associated indicators of compromise.

Service Reviews

One per quarter, Exium provides a formal service performance assessment, which includes a review of XDR service performance, major events and incidents, faults, change requests and implementation, and recommendations for improvement.

Single, integrated and automated platform for complete visibility

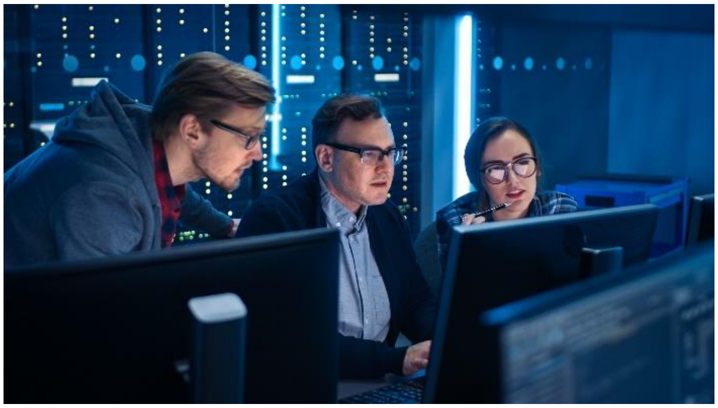
Exium XDR unifies detection and response across your security stack. Exium and non- Exium telemetry are integrated into one single command console for unified detection and response. Exium XDR turns cryptic signals trapped in siloed solutions into high-efficacy, real-time detections and deep investigation context. Equipped with Exium XDR, security professionals can more quickly and intuitively investigate, threat hunt and respond.

An analytics engine fed by native, intelligent sensors offers more effective security analytics than can otherwise be achieved on top of third-party products and telemetry. Any given vendor will have a much deeper understanding of their own solutions' data than a third-party's data.

Exium XDR works in tandem with our SASE (Secure Access Services Edge), endpoint and cloud security solutions to provide organizations a more comprehensive view of their risks and a more holistic approach to securing against and remediating threats.

Exium XDR Benefits	
Enterprise-wide visibility	Gain visibility across network, endpoint, and cloud data. Collect and correlate data from Exium and third-party tools to detect, triage, investigate, hunt, and respond to threats. Having full visibility across your system, including on-premises and in the cloud enables you to detect and block attacks faster.
Behavioral analytics	Accurately detect evasive threats by profiling user and endpoint behavior as well as identifying anomalies indicative of attacks.
AI-based malware analysis	Examine files with an adaptive local analysis engine that's always learning to counter new attack techniques.
Integrated threat intelligence	XDR incorporates information on known attack methods, tools, sources, and strategies across multiple attack vectors. Threat intelligence enables XDR to learn from attacks on other systems and use that information to detect similar events in your environment.
Block known and unknown attacks	XDR centralizes security events across multiple security controls to provide a holistic approach to security. The solution combines weak security signals from multiple sources into stronger signals to identify known and unknown threats.
	Machine learning-based detection includes supervised and semi-supervised methods that work to identify threats based on behavioral baselines. Machine learning technologies enable XDR to protect against malicious insiders, policy violations, external threats, ransomware, advanced zero-day malware, and non-traditional threats that can bypass signature-based methods.

Automatically protect against sophisticated attacks	
Avoid alert fatigue	Convert a large stream of alerts into a much smaller number of incidents that can be focused on for investigation. Further simplify investigations with automated root cause analysis and a unified incident engine, lowering the skill required to triage alerts. Data without context is nothing more than meaningless noise. Without an integrated platform to correlate data, security analysts are buried in an overwhelming volume of alerts. With greater context, XDR eliminates false positives to enable security operations to focus on incidents that matter.
Effective Response orchestration	Response orchestration capabilities enable response actions directly through XDR interfaces, as well as communication between tooling. For example, XDR can update network policies across the enterprise, in response to an automatically blocked attack on a single network. Robust data collection and analysis allows you to trace an attack path and reconstruct attacker actions. This provides the information needed to locate the attacker wherever they are. It also provides valuable information that you can apply to strengthen your defenses.
Hassle-free detections and investigation	XDR enables more insightful investigations because you can make logical connections from the data provided within a single view. XDR augments security analysts' capabilities and streamlines workflows. It optimizes teams' efforts by speeding up or removing manual steps and enables views and analyses that can't be done immediately. Analysts and threat hunters can focus on high-priority threats because XDR weeds out anomalies determined to be insignificant from the alert stream.
Increased Productivity	XDR reduces the number of alerts and increases alerting accuracy. This means fewer false positives to sift through. Also, since XDR is a unified platform and not a combination of multiple point solutions, it is easier to maintain and manage, and reduces the number of interfaces that security must access during a response. Because XDR not just detects but also responds to threats, a security team could save time and resources with XDR implementation.



Ready to put your Security Operations on Autopilot?

Test Drive Here