

Your Unified Security Solution



XDR is a comprehensive threat management solution that unifies prevention, detection, and response across your entire environment in a seamless, human-led service-technology offering. Powered by static AI, machine learning, automation, custom tuning, and human investigation and remediation capabilities to stop even the stealthiest attacks, XDR gives you 24x7x365 protection across all major threat vectors. This Extended Detection and Response solution begins with rapid elimination of threats through automated processes, adds policy-driven response capabilities, and ultimately gives complete visibility with full-context, real time forensics.

Beyond Automated Response

Once automated process have been executed, certified security analysts evaluate security information from across your environment for event identification, remediation, and proactive threat hunting, giving you true assurance 24x7x365. Our certified professionals will help you streamline your audit and security documentation for simplified updates, reporting, and team task management.

Our Open XDR platform leverages:

- Endpoint Security Monitoring
- Network Security Monitoring
- Firewall Security Monitoring
- Platform as a Service Monitoring (Microsoft 365, G-Suite, etc.)
- SaaS Platform Event Monitoring (SaaS stacks – Azure AD, Salesforce, etc.)
- Cloud Security Event Monitoring
- Dark Web Monitoring
- DNS Monitoring

XDR not only keeps you **secure**, but **simplifies** your life.



480-389-3444 | [cisco.inc](https://www.cisco.com)

Common Problems XDR Solves:

Lack of visibility across environment.

Understanding the full scope of an attack requires broad visibility and telemetry. XDR pulls security information from across your environment, enabling automated responses and event correlation that quickly give our analysts the big picture.

Endless games of whack-a-mole. Today's attackers have evolved stealthier tactics, often navigating quietly to harder-to-watch parts of your environment while you're still reviewing

obvious alerts. XDR pulls all the security data together for quick, accurate understanding of what's really happening.

Too many tools to manage. Disparate toolsets require not only better integration, but always-available cyber talent that is dedicated only to monitoring & response. Because this is typically unrealistic, XDR stitches together your security tools, custom processes, and our people for a comprehensive solution.

STRATEGY & RISK

- Gap Analysis
- Audit/Assessment
- Third Party Risk Management
- FedRAMP
- StateRAMP
- CMMC
- Advisory
- Virtual CISO
- Managed Compliance
- Managed GRC

CYBER DEFENSE OPERATIONS

- Extended Detection & Response
- Managed Detection & Response
- SIEM as a Service
- Threat Hunting
- Cyber Threat Intelligence
- Digital Forensics
- Vulnerability Management Program
- Attack Surface Reduction
- Cyber Incident Response

SECURITY ARCHITECTURE & ENGINEERING SOLUTIONS

- Secured Managed Services
- Advanced Firewall Management
- Identity & Access Management
- Cloud Security
- Data Protection
- Remediation

READINESS & RESILIENCY

- Penetration Testing
- Tabletop Exercises with Incident Response Retainer
- Training Programs

CISO



SOC 2® Type II Audited



480-389-3444 |

ciso.inc