

Cisco XDR

Security Operations Simplified

September 2023

Contents

Cisco XDR Product Overview	3
Security Operations Simplified	3
Use Cases	4
Accelerate Incident Responses with Streamlined Workflows and Prioritization	4
Automation – No SOAR Required	4
Conduct Truly Extended Detection and Response	4
Key Capabilities	5
Security Analytics and Correlation	5
Network Telemetry Ingestion	5
Asset Context	6
Incident Prioritization	6
Incident Response	6
Threat Intelligence	6
Threat Hunting	7
Custom Automation Workflows	7
Automation Workflow Exchange	7
Integrations	8
Email Telemetry and Response Integrations	8
Endpoint (EDR) Telemetry and Response Integrations	8
Network Detection and Response (NDR) Integrations	8
Next-Generation Firewall (NGFW) Telemetry and Response Integrations	9
Security Information and Event Management (SIEM) Integrations	9
Application, Identity, and Device Management Integrations	9
Cloud Security Integrations	9
Public Cloud Integrations	10
Threat Intelligence and Threat Hunting Integrations	10
License options	11
Third-Party Telemetry	11
Cisco Secure Managed Detection and Response	12
Cisco Talos Incident Response Retainer Service	12
Cisco Technical Security Assessment	12
Support	13
Cisco XDR Software Support Service	13
Cisco Software Support Enhanced (included)	13
Cisco Software Support Premium (add-on)	13

Cisco XDR Product Overview

Security Operations Simplified

Cisco XDR simplifies security operations, accelerates responses, and empowers Security Operations Center (SOC) teams with AI-driven and proactive threat detection and response. It is designed to address the challenges faced by security analysts and offers a cloud-native, extensible solution that brings data from multiple security tools, and applies machine learning and analytics to arrive at correlated detections.

By moving beyond endpoint detection and response (EDR) or Security information and event management (SIEM) centric approaches, Cisco XDR shifts the focus from endless investigation to remediating the highest priority incidents with evidence backed automation, helping SOC teams act with greater speed, efficiency, and confidence. While traditional SIEM technology provides management for log-centric data and measures outcomes in days, Cisco XDR focuses on telemetry-centric data and delivers outcomes in minutes.

Cisco XDR natively analyzes and correlates the six telemetry sources that Security Operations Center (SOC) operators say are critical for an extended detection and response (XDR) solution: endpoint, network, firewall, email, identity, and DNS. With Cisco XDR, security teams can detect threats beyond the endpoint by making telemetry and insights from other sources, including the network equally foundational. Through turnkey, curated integrations with third-party security products as well as the extensive Cisco Security solutions portfolio, Cisco XDR delivers a seamless installation into existing architectures and delivers consistent outcomes regardless of vendor or solution.

Cisco XDR correlates telemetry, rather than just aggregating data. By doing so, it reduces false positives and delivers prioritized incidents based on potential risk and impact to your environment. In other words, it lets your teams focus on the threats that matter. And it enriches detections with threat intelligence from Talos to add context and asset insights, ensuring you are always seeing the complete picture.

By doing XDR right, security teams can confidently respond to attacks, increase SOC efficiency, and automate tasks for a more proactive approach to security.

Cisco XDR is designed to deliver greater efficacy, better experience, and greater return on investment from your existing security stack through four key value pillars:

1. **Detect the most sophisticated threats:** You can investigate every corner of your environment by connecting the broad end-to-end Cisco security portfolio as well as select third-party tools. Also, by providing the underlying threat intelligence from Talos to enrich incidents with added context and asset insights, we can detect and respond to the most sophisticated threats impacting a wide security stack, regardless of vendor or vector.
2. **Act on what truly matters, faster:** Prioritize the threats that pose the greatest material risk to your business. Unified context to streamline investigations, and evidence-backed recommendations.
3. **Elevate productivity:** Filter out the noise so that your analysts focus on what truly matters. Boost limited resources for maximum value. Automate tasks and focus on strategic tasks.
4. **Build security resilience:** Close security gaps. Anticipate what's next through actionable intelligence. Get strong every day with continues, quantifiable improvement.

For more information, go to cisco.com/go/XDR.

Use Cases

Accelerate Incident Responses with Streamlined Workflows and Prioritization

By conducting the investigative process for you, Cisco XDR eliminates work effort on the part of Level 1 and Level 2 analysts, allowing incident response to begin immediately. Cisco XDR then provides clear guidance on the appropriate response to take based on the incident experienced, so analysts can act immediately to prevent further impact and eradicate the incident in your environment. Finally, by prioritizing incidents based on the material risk to your organization associated with respective MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) and the value of the affected assets, Cisco XDR ensures that your organization focuses on the potentially most impactful incidents.

Automation – No SOAR Required

Detection without response is insufficient, so response capabilities need to be built into an XDR solution. Enhancing this standard, Cisco XDR includes expertly curated automation and orchestration, extending response capabilities to automated workflows, reducing the effort required by SOC teams and analysts. When organizations need to expand on the built-in capabilities provided out-of-the-box by Cisco XDR, they can create and save customized workflows for executing their common SOC processes.

Conduct Truly Extended Detection and Response

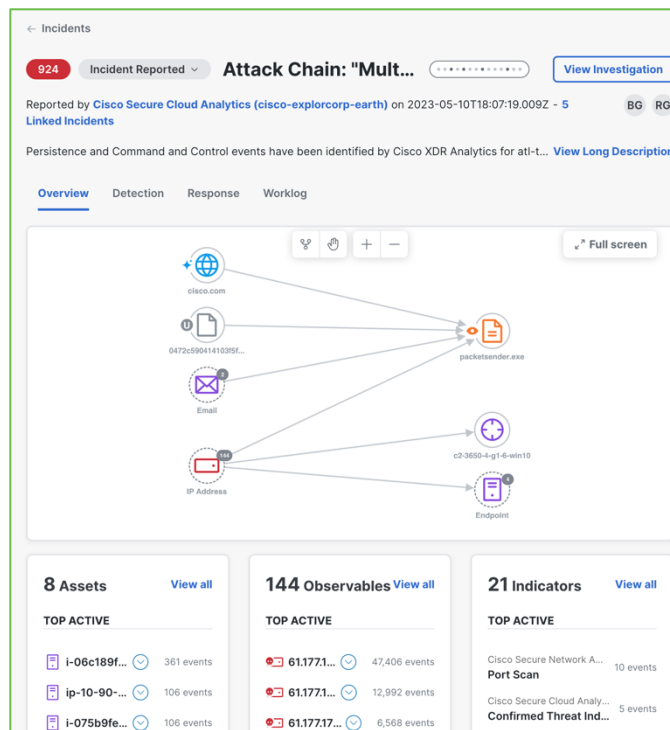
How can you possibly evaluate incidents and threats to your environment if you are not doing so across all possible vectors, security data sources, non-security pertinent data sources, and countermeasures? Cisco XDR delivers native integrations with Cisco security solutions as well as non-Cisco tools across key vectors of endpoint, email, cloud, and network. Cisco XDR provides and maintains Cisco-curated integrations for market-leading third-party security countermeasures in endpoint, email, cloud, firewall, and network through established development agreements with these key partners, offloading the requirement for your organization to do so, to fully leverage your technology investments.

Key Capabilities

Security Analytics and Correlation

Cisco XDR has a built-in analytics and correlation engine (i.e., Cisco XDR analytics), which can ingest a vast variety of events and telemetry. This ranges from EDR security events to public cloud and private network flow logs and more. It is possible to ingest both Cisco and third-party data into Cisco XDR analytics (depending on license tier).

This analytics engine provides users with fully correlated incidents based on a variety of detections and correlation mechanisms. Security events are correlated over time revealing the bigger picture of a multi-stage attack. Incident activity is plotted on a timeline and visualization is provided by an attack graph, so that the analyst quickly understands the who, what, where, when of an attack. Incidents are assigned a priority score on a scale from 0 to 1000 that reflects the risk associated to the detection, which is related to the material risk associated with respective MITRE ATT&CK TTPs and the value of the affected assets. This incident also correlates related alerts based on common indicators to show the entire attack mapped to the MITRE ATT&CK framework.



Network Telemetry Ingestion

Security operations teams often face “blind spots” within their environments as the number of user devices on the private network grows and more workloads shift to the public cloud. Many attacks require adversaries to interact with the network to achieve their goal. Cisco XDR analytics can collect network traffic from on-premises networks and public clouds to identify hosts, build an understanding of normal host behavior, and generate alerts when device behavior changes in a manner that is relevant to an organization’s network security. These alerts subsequently feed into the incident correlation process and are used for attack chains.

Cisco XDR can ingest public cloud logs (AWS, Google Cloud Platform, and Microsoft Azure) using an agentless monitoring of workloads and API integrations to deliver threat detection and configuration monitoring. It integrates with additional Cloud Service Provider APIs (for example in AWS with Cloud Trail, Cloud Watch, Config, Inspector, Identity and Access Management [IAM] Lambda, and many more) to look for adversary behavior on the network and infiltrating deep into an organization’s cloud environment.

To monitor on-premises networks, Cisco XDR includes **Cisco Telemetry Broker (CTB)**, which can ingest network telemetry from many sources, like flow data (e.g., NetFlow, IPFIX, etc.), SPAN/mirror port traffic, and NGFW log information. CTB is pre-configured to send all telemetry from Cisco XDR to the SaaS-based data repository where this data is stored, analyzed, and correlated with all other available telemetry.

Cisco XDR also includes the **Network Visibility Module (NVM)** that can be directly deployed using cloud-managed Cisco Secure Client (formerly AnyConnect). NVM delivers a continuous feed of high-value endpoint telemetry which allows organizations to see endpoint and user behaviors on their networks. It collects flow logs directly from endpoints on- and off-premises, and valuable contexts like users, applications, devices, locations, and destinations. NVM telemetry can be crucial in correlating network telemetry with endpoint process information, as it contains both on a single log line.

Asset Context

The Cisco XDR Insights feature extends the integration framework to collect data about device inventory and posture. A unique combination of data from security products and traditional device managers results in a unified asset inventory that can be used to provide context to investigations and meaningful reports. Each device has a single page of information about it, merged from all sources. It also allows defining a device's "value" which is used when scoring XDR incidents. If incidents contain assets, they will be visible when reviewing, investigating, and responding to the incident.

Incident Prioritization

New incidents are assigned a priority score and are automatically enriched. New detections that are discovered in the enrichment process that are relevant to an incident are added to that incident. The incident priority score (0-1000) used to prioritize incidents is made up of Detection Risk (0-100) and Asset Value (0-10). The Detection Risk score is composed of the MITRE TTP financial risk, number of MITRE TTPs, and source severity. The Asset Value is a user defined value, which represents the value of the asset involved in the incident.

After an incident is prioritized, it shows up in a list form, sorted by priority score, enabling analysts to quickly decide what to investigate first and focus on the incident with the highest priority score. Various options for sorting, filtering, assignees, and status can be changed directly in the incident list.

The screenshot displays the Cisco XDR Incidents interface. On the left, a list of incidents is shown, sorted by priority. The list includes columns for checkboxes, priority scores, names, and sources. The right pane shows the details for a specific incident titled "Geographically Unusual Remote Access for Cisco - ...". This pane includes a priority score of 1000, a status of "Incident Report...", and a short description: "Geographically Unusual Remote Access on i-0c6069f352916581e". It also features a long description with an alert, tenant information (Cisco - Lawrenceville Lab (Earth)), and source information (i-0c6069f352916581e). A "View Incident Detail" button is located at the bottom right of the right pane.

Priority	Name	Source
1000	EC2AM...	Secure E...
1000	Geogra...	Cisco Se...
1000	Heartbe...	Cisco Se...
1000	c4-365...	Secure E...
1000	c5-930...	Secure E...
924	Attack ...	Cisco Se...
873	c1-450...	Secure E...
783	c3-930...	Secure E...
765	Persiste...	Cisco Se...
523	c1-450...	Secure E...
392	c1-930...	Secure E...

Incident Response

When an incident is created, prioritized, and enriched, it is critical to quickly respond to a breach. The built-in Response Playbook allows security analysts and incident responders to do this. Contextual playbooks provide a step-by-step, guided response for incidents that follows the SANS "PICERL" incident response model. Many actions in the playbook are powered by native XDR Automation workflows. These workflows take actions based on which products you have integrated accelerating how you respond. The incident's Worklog allows you to view work already completed for the incident, post notes with important details, and collaborate with your team. You can also review the history of actions taken, including the execution of automated response actions in the response playbook.

Threat Intelligence

In the Cisco XDR platform, it is possible to combine multiple sources of threat intelligence in addition to the built in Cisco Talos intelligence. This offers crucial context during enrichment of incidents, or while doing threat hunts. This threat intelligence can include simple reputations, or more complex relationships between attack tools, techniques, and known threat actors. Users can enable multiple Cisco and third-party intelligence providers and access all of them in unison natively in investigations through the Cisco XDR Investigate feature. (Third-party integrations are supported at the Advantage and Premier license levels.)

Threat Hunting

With the Cisco XDR Investigate feature, it is possible to do advanced threat hunting with a comprehensive, yet simple user experience. While doing an investigation, Cisco XDR will query all integrations, retrieving both local and global threat intelligence as well as any reported sightings of the investigated items in your environment. This is then normalized into the CTIM data model. After this, it is possible to see a graph view of all the artifacts you are investigating, with an adjustable timeline. You can also use graph filters and a table view to quickly focus on specific items. It is possible to start an investigation based on an existing incident, a set of observables, or even by copy pasting a piece of text (e.g., a blog post). Using the rich Cisco XDR APIs, it is even possible to do an investigation completely automated.

Custom Automation Workflows

Cisco XDR Automation provides a no-to-low code approach for building automated workflows. These workflows can interact with various types of resources and systems, whether they're from Cisco or a third-party vendor. Automation workflows are the parent component and are like a script in traditional programming. A workflow can be simple and have only a few actions, or complex and string together many different actions for different products. Using the drag-and-drop interface, it is possible to create your own workflows, which can be triggered by a variety of schedules and events. Examples are new incidents, an email received, a webhook executed, schedules, and more. Automation Rules allow you to manage all workflows and triggers in a single holistic experience.

Triggers

To add a trigger to a workflow, configure an automation rule that determines when a workflow is executed, such as when an incident, specific event occurs, or on a schedule.

Automation Rules Events Webhooks Calendars Schedules

Search

Type

Q Search X

Select

Reset All

Display name	On/off	Type	Owner
Hourly Workflow	<input type="checkbox"/>	Schedule	user@cisco.com
Incoming Webhook	<input checked="" type="checkbox"/>	Webhook	user@cisco.com
Incident Notification	<input checked="" type="checkbox"/>	Incident	user@cisco.com

Automation Workflow Exchange

The Cisco XDR Automation Exchange allows you to quickly find new automation workflows and install them through an installation wizard. This allows you to quickly discover new curated content and operationalize it within a few clicks. On the Exchange page, you can easily locate useful workflows and streamline the workflow import process using the 1-Click Install wizard. It is possible to filter Exchange by products, as well as view popular workflows.

Integrations

The following is a list of integrations supported by Cisco XDR, all of which are cloud based. Product names with the 'N' designation are native Cisco integrations, those with a 'C' are Cisco-curated integrations of third-party products, both of which are supported out-of-the-box. The products without a designation are solutions that likely can be integrated into Cisco XDR by the customer but may not have been tested and validated. This list is representative, does not guarantee that the solutions listed here will successfully integrate with Cisco XDR, is not intended to be complete, and is subject to change at any time without notice.

Email Telemetry and Response Integrations

These integrations provide understanding of email as a threat vector by visualizing message, sender, and target relationships in the context of a threat. Email integrations provide tiles to Control Center, as well as actions for orchestration, so practitioners can build automated workflows, helping to obtain better context of a threat to combat phishing attacks, business email compromise, malware, and ransomware.

- Cisco Secure Email and Web Manager ^N
- Cisco Secure Email Gateway ^N
- Cisco Secure Email Threat Defense ^N
- *Microsoft Defender for Office 365 ^C – Coming soon*
- *Proofpoint Email Protection ^C – Coming soon*

Endpoint (EDR) Telemetry and Response Integrations

EDRs provide a list all managed endpoints and their details are extracted and stored within a centralized location of Cisco XDR, allowing for devices to be uniquely identified and acted upon without depending on unreliable IP addresses. Endpoint context allows investigation on files and processes matching a SHA256 hash across and URLs these key data points are correlated to promote week alerts to high efficacy incidents. They are essential for taking response steps (one-click or fully automated) to mitigate, contain, eradicate, or recover from an attack.

- Cisco Secure Endpoint ^N
- CrowdStrike Falcon® Insight ^C
- Cybereason Endpoint Detection and Response ^C
- Microsoft Defender for Endpoint ^C
- *Palo Alto Networks Cortex ^C – Coming soon*
- SentinelOne Singularity™ ^C
- Trend Vision One ^C

Network Detection and Response (NDR) Integrations

NDR is a core foundational integration of Cisco XDR as it enriches threat detection with agentless behavioral and anomaly detection capabilities and unique network device context. It can be combined with sources of global threat intelligence and internal visibility to develop confirmed threat alerts based on known incidents of compromise. NDRs also offer a rich set of network device context which is essential to ascertain incident criticality. This historical network data is queried by Cisco XDR to enrich threat hunting and forensic audits and XDR incidents, simplifies visibility, and increases response efficiency.

- Cisco Secure Cloud Analytics ^N
- Cisco Secure Network Analytics ^N
- *Darktrace Respond & Detect ^C – Coming soon*
- *ExtraHop Reveal(x) 360 ^C – Coming soon*

Next-Generation Firewall (NGFW) Telemetry and Response Integrations

The integration of NGFW devices provides sightings of IP addresses, URLs, and domains as additional context and to further forensic investigations in Cisco XDR. Additionally, users can leverage Secure Firewall to block IPs at the perimeter. Secure Firewall devices can also be configured to provide alerts to Cisco XDR to be triaged and correlated, displaying the most pressing alerts in the Cisco XDR incident manager. The querying of all configured firewall devices to enrich observables related to an XDR incident improves visibility and understanding of attacks. Combined with automated response capabilities and using them in coordinated, single-click defenses simplifies visibility and increases response efficiency.

- Cisco Secure Firewall ^N
- Check Point Quantum Security Gateway and Management ^C – Coming soon
- Fortinet FortiGate ^C – Coming soon
- Palo Alto Networks NGFW ^C – Coming soon

Security Information and Event Management (SIEM) Integrations

Cisco XDR can utilize SIEMs to query threat response for targets and verdicts from observables using built-in enrichment or through manual investigations. Supported observable types include IPv4 addresses, IPv6 addresses, domains, file names and SHA256 file hashes. These integrations enable an investigator to collect Sightings from many data sources, by using the integration as a translation layer between data models withing Cisco XDR workflows.

- Microsoft Sentinel ^C – Coming soon
- Devo
- Exabeam
- Google Chronicle
- Graylog
- LogRhythm
- Splunk
- Sumo Logic Cloud SIEM
- Sumo Logic Log Management

Application, Identity, and Device Management Integrations

These sources have their own inventories of devices or device objects, and these integrations bring information about these devices into a centralized location within Cisco XDR. This comprehensive view provides the data and context needed to better identify vulnerabilities, prevent threats, and prioritize remediations.

- Cisco Duo ^N
- Cisco Identity Services Engine ^N
- Cisco Orbital ^N
- Cisco Secure Web Appliance ^N
- Cisco Umbrella ^N
- Microsoft Azure AD ^C – Coming soon
- Ivanti Neurons
- Jamf Pro
- Meraki
- Microsoft Intune
- SpyCloud Account Takeover Prevention
- VMWare Workspace ONE UEM

Cloud Security Integrations

Cloud security integrations are valuable in reducing security and compliance risks, managing security policies across multiple products, determining which vulnerabilities pose the highest risk and which can be deprioritized, and securing applications in hybrid work environments. Additional capabilities from these integrations include protection against DDoS threats and OWASP attacks and extending web security.

- Cisco Attack Surface Management ^N
- Cisco Defense Orchestrator ^N
- Cisco Secure Cloud DDoS Protection Service ^N
- Cisco Secure Cloud WAF Service ^N
- Cisco Secure Workload ^N
- Cisco Vulnerability Management ^N (formerly Kenna)
- Akami
- Microsoft Graph Security API
- Signal Sciences Next-Gen WAF

Public Cloud Integrations

Integrate Cisco XDR with the leading Public Cloud providers to gather network meta data from Flow Logs, proprietary logs and APIs providing a powerful source for entity modeling, baselining, and detecting malicious network activity. Entity modeling uses flow meta data to build a model of normal activity from observed device behavior and uses this model to spot changes in behavior that may be due to misuse, malware, or compromise. By integrating cloud providers, Cisco XDR helps security operation centers (SOCs) stop chasing cybercriminals and their never-ending myriad of exploits, malware, and other threats by trying to keep up with their signatures. Instead, the SOC can focus security efforts on a small, prioritized number of significant and automatically detected deviations from established patterns and activities, as identified by entity modeling.

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Threat Intelligence and Threat Hunting Integrations

Access to numerous threat intelligence sources is included with Cisco XDR at no additional cost. These include the Talos database, the default Cisco Threat Intelligence Architecture, and a private repository into which users can upload their own threat intelligence, whether generated in house or acquired from other sources. Integration of Secure Malware Analytics within Cisco XDR allows users to get detailed intelligence about malware, associated network traffic, system changes, and more to gain heightened malware threat intelligence via automated detonation of suspected files from a global user base.

- | | |
|--|--|
| • Cisco Secure Malware Analytics ^N | • IBM X-Force Exchange (threat intelligence) |
| • Cisco Talos Intelligence ^N | • IsItPhishing (threat intelligence) |
| • Cisco Threat Intelligence API ^N | • MISP (threat intelligence) |
| • AbuseIPDB IP Checker (threat intelligence) | • Palo Alto Networks AutoFocus (threat intelligence) |
| • AlienVault Open Threat Exchange (threat intelligence) | • Pulsedive (threat intelligence) |
| • alphaMountain.ai Threat Intelligence (threat intelligence) | • Quals IOC (threat hunting) |
| • Amazon GuardDuty (threat detection) | • Recorded Future (threat intelligence) |
| • AMP File Reputation ^N (threat intelligence) | • SecurityTrails (threat intelligence) |
| • APIVoid (threat intelligence) | • ServiceNow SecOps (threat intelligence) |
| • Censys (threat intelligence) | • Shodan (threat intelligence) |
| • CyberCrime Tracker (threat intelligence) | • Sixgill Darkfeed (threat intelligence) |
| • Farsight Security DNSDB (threat intelligence) | • Threatscore Cyberprotect (threat intelligence) |
| • Google Safe Browsing (threat intelligence) | • ThreatQuotient (threat intelligence) |
| • Have I Been Pwned (threat intelligence) | • urlscan.io (threat intelligence) |
| | • VirusTotal (threat intelligence) |

License options

There are three License tiers in which Cisco XDR is available: Essentials, Advantage, and Premier (licensed per user).

Cisco XDR Essentials delivers the full XDR features and integrates across the Cisco Security portfolio, with a few exceptions. **Cisco XDR Advantage** builds upon the capabilities delivered in Essentials by adding Cisco-curated integrations with select third-party security tools. **Cisco XDR Premier** delivers the full Advantage capabilities as a Managed Service provided by Cisco security experts and includes security validation through penetration testing and select Cisco Talos Incident Response services.

Table 1. Cisco XDR License Options

Features	Essentials	Advantage	Premier
Security Analytics and Correlation	✓	✓	✓
Threat Intelligence	✓	✓	✓
Threat Hunting	✓	✓	✓
Incident Response Actions	✓	✓	✓
Incident Prioritization	✓	✓	✓
Case Prioritization	✓	✓	✓
Asset Context	✓	✓	✓
Custom Workflows	✓	✓	✓
Automation Workflow Exchange	✓	✓	✓
Data Ingestion / Data Retention	✓	✓	✓
Cisco Software Support Enhanced	✓	✓	✓
Third-Party Telemetry		✓	✓
Cisco Secure Managed Detection and Response			✓
Cisco Talos Incident Response (Talos IR)			✓
Cisco Technical Security Assessment (CTSA)			✓

Data retention: A data retention period of 90 days is included by default. Customers can purchase additional retention periods of 180 or 365 days.

Data ingestion: Each tier includes a data ingestion limit of 2GB per user per month. Customers can purchase additional GBs beyond the 2GB default, measured in units of GB per user per month.

Third-Party Telemetry

Cisco XDR Advantage customers will benefit from commercially supported and curated integrations with select third-party tools across a range of vectors, including endpoint detection and response (EDR), email threat defense (ETD), next-generation firewall (NGFW), network detection and response (NDR), and security information and event management (SIEM). The list of third-party integrations supported and curated by Cisco is dynamic, so please speak with your Cisco representative for the current list.

Cisco Secure Managed Detection and Response

The Cisco XDR Premier license tier is a managed detection and response (MDR) service using the Cisco XDR solution provided by Cisco security experts. It includes security validation through penetration testing and select Cisco Talos Incident Response Retainer Services. Cisco Secure MDR powered by Cisco XDR service uses a combination of Cisco's team of researchers, investigators, and responders, the Cisco XDR solution, integrated tool sets, and additional Cisco security technologies (where available) to monitor for and respond to potential security threats and breaches.

The Cisco Secure MDR powered by Cisco XDR service includes:

- **24x7x365 monitoring:** Global security incident and alert monitoring by expert security investigators.
- **Unmatched Cisco expertise:** Cisco's team of researchers, investigators, and responders leverage both Talos Threat Intelligence and defined investigation and response playbooks to help detect, investigate, and respond to threats and alerts. Cisco's responses may include additional information, recommendations, or changes based on the type of threat or indication of compromise.
- **Quarterly threat briefings:** The Cisco Secure MDR intelligence team hosts remote review meetings on a quarterly basis open to all MDR customers, co-delivered by Cisco Talos Incident Response. This quarterly briefing provides updates on current threat patterns, detection volumes, and trending events.
- **Dedicated service portal:** The dedicated Cisco Secure MDR powered by Cisco XDR service portal provides security incident lifecycle management, dashboards metrics, knowledge base, SOC communication, and more.
- **Threat advisories:** Cisco Secure MDR powered by Cisco XDR issues threat advisories for new threats discovered helping customers to proactively prevent incidents or compromises through the implementation of mitigating controls. All past intelligence articles and advisories are available from the MDR powered by Cisco XDR Portal Knowledge Base.

Cisco Talos Incident Response Retainer Service

Cisco Talos Incident Response Retainer Service provides a full suite of proactive and emergency incident response services to help you prepare, respond, and recover from a cybersecurity incident. With this flexible service, you benefit from:

- **Incident response expertise:** Our global team of seasoned incident responders is available during active incidents and to help strengthen your overall defenses.
- **Swift action:** One of our incident responders can be remotely dispatched within four (4) hours of reporting an active incident, which minimizes downtime and accelerates incident resolution.
- **Intelligence-enriched analysis:** Driven by an evergreen library of threat intelligence and backed by proven incident response processes.

Cisco Technical Security Assessment

Cisco Technical Security Assessment provides a suite of proactive services to assess a customer's cyber security posture and advice on the threats they face, the likelihood of those threats being realized, and the impact on their operational resilience if they are. This includes but is not limited to:

- Threat Modelling
- Penetration Testing
- Red Team Threat Simulation
- Security Architecture Assessment
- Application Security Assessment
- Security Operations Assessment
- Development Operations Security Assessment
- Device Configuration and Build Reviews

Support

Cisco XDR Software Support Service

There are two levels of support available:

- **Cisco Software Support Enhanced** is included with all Cisco XDR License Tiers at no additional cost
- **Cisco Software Support Premium** is available for purchase at an additional fee

Cisco Software Support Enhanced (included)

- Solution Support (Reactive Technical Support):
24x7 with 30-minute response time service level objective (SLO)
- Onboarding guidance
- Ongoing digital adoption
- Periodic Security Health Checks: One (1) per year for the covered environment

Cisco Software Support Premium (add-on)

- Cisco Software Support Enhanced
- Designated Customer Success Point of Contact
- Extended adoption sessions: Up to six (6) adoption sessions per year
- Periodic business and success review

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)