Trend Micro™ Worry-Free™ Co-Managed XDR: Cybersecurity Incident Response Guide

Introduction to Trend Micro™ Worry-Free™ Co-Managed XDR Service

Trend Micro™ Worry-Free™ with Co-Managed XDR is a cross-product, cross-customer, and cross-partner cybersecurity detection and response service, co-managed by Trend Micro and Managed Service Providers (MSPs), helping to mitigate threats for customers while alleviating overburdened MSPs. Using Trend's expertise, MSPs can now elevate their security offerings, protect customers against ransomware, malware, and other malicious activity without additional resources and investment.

There are many options when it comes to selecting a security vendor or adding a security vendor to an existing technology stack. Trend views the MSP partnership as more than just product and economics. It is about closing security gaps, open communication, long-term focus on people and partnerships. As experts in security and an advocate for MSPs, the focus is on supporting customers and building confidence in security offerings.

Worry-Free with Co-Managed XDR allows MSPs to offer a consistent level of security to customers, at scale with holistic threat visibility and correlation across endpoint and email, enabling proactive containment and intelligent response by Trend's threat experts while MSPs maintain control over the interactions with customers. As part of the incident response service, Trend's 24/7 threat experts provide customized recommendations or remediation actions, if authorized.

Additionally, this service provides proactive threat assessments across the MSP's entire customer base and protects multiple customers at once. Taking it one step further, our security analysts review similar threats across global partners, especially those in the same industry, to provide proactive response.

Worry-Free with Co-Managed XDR provides visibility, recovery, response and security confidence that reduces customers cybersecurity risks.

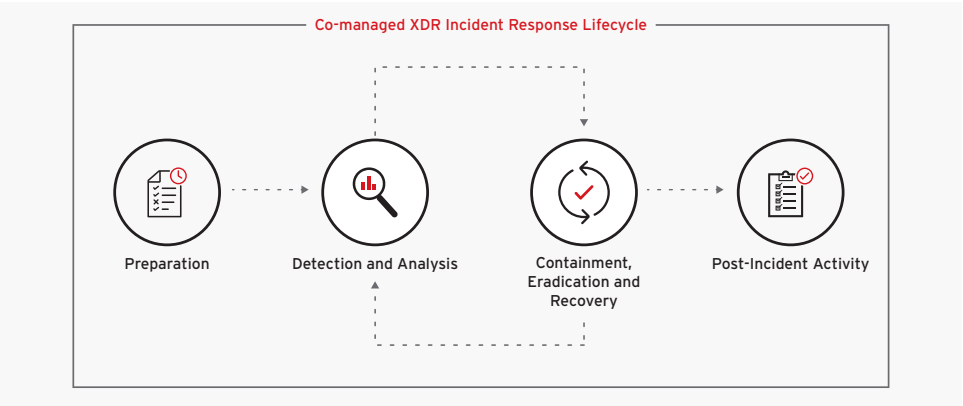
MSP's responsibilities are to:

- Attend all Trend's internal threat-related trainings.
- Familiarize themselves with the co-managed XDR service and processes.
- Learn how to use the XDR tools and features within the Worry-Free platform.
- Understand the importance of data confidentiality/privacy of their customers.
- Provide Primary and Secondary emergency contact person after initial onboarding. This contact information will be used in case of breach or attacks.

Worry-Free Cybersecurity Incident Response Plan (CIRP)

The Worry-Free Cybersecurity Incident Response Plan (CIRP) is a set of procedures and guidelines based on the NIST Incident Response Lifecycle and designed for MSPs to understand the steps that the Worry-Free co-Managed Service Team takes to detect, analyze, contain, eradicate, and recover from a cyber-attack or security breach.

The purpose of this CIRP is to minimize the impact of a cybersecurity incident on an organization's operations, reputation, and financial stability. The plan is customized to the specific needs of the organization and takes into account its risk profile, critical assets, and business continuity requirements.



Worry-Free with Co-Managed XDR is aligned with the NIST (National Institute of Standards and Technology). This lifecycle closely covers a broad base, from preparing for an attack to making sure an incident is not repeated.

I. Preparation

Trend's Co-Managed XDR Service Team consists of security analysts and product experts who are trained to address security incidents and to know the procedures to identify, isolate, and remediate cyber threats.

Under the Worry-Free Co-Managed XDR service, Trend will be responsibility for:

- Training the MSP to handle and analyze different types of threats.
- Keeping the CMST's security analysts aware of latest threats and news about cybersecurity.
- Conduct Tech Shares to improve the knowledge/skills of Security Analyst.
- Integration of MSP into the Co-Managed XDR service program
- Create high quality XDR alerts. The Global Threat Intelligence of Trend Micro™ Smart Protection Network™ and Expert Detection Rules produced by Trend's threat experts maximize the power of artificial intelligence and analytical models. We apply it to the activity data collected from the environment's sensors to produce higher fidelity alerts, enabling holistic visibility and analysis.
- Provide Best Practices Guide and recommendations. After the onboarding, we will provide a set of links and resources to follow set by Trend to make sure that they are not only leveraging all the protection features but also to make sure the customer's telemetry data are monitored properly.
- Perform quarterly policy assessments to review configuration for Worry-Free products based on best practices.
- Create, maintain, and enhance documentations and playbooks.
- Automatically monitor all the Partner's customers with Co-Managed XDR license *(including those newly added/ assigned customers).*

	RESPONSIBILITY	
	TREND MICRO	MSP
Onboarding and Training:		
Attend and complete Trend's security trainings	○	●
Familiarize with the processes of the co-managed XDR service	○	●
Learn how to use the tools/platforms that are utilized in the service	○	●
Learn how to handle and analyze different types of threats	○	●
Provide best practices guide and recommendations	●	
Security and Management:		
Deploy co-managed XDR services into customers environment		●
Create high-quality XDR Alerts	●	
Monitor customers associated with co-managed XDR license	●	
Create, maintain, and enhance documentations and playbooks	●	
Quarterly policy assessment report	●	
Review customers telemetry data is being monitored properly	●	

○ Limited Responsibility ● Full Responsibility

II. Detection and Analysis

The identification phase of an incident response plan involves determining whether an organization has been breached. This phase also includes the investigation of the depth of the compromise, its source, and its success or failure. The Co-Managed XDR Service Team has a process to determine a breach, detect anomalies/infection, and can perform the following actions to identify the scope of the incident.

1. Detect

- Product correlation is performed using different sensors with the help of XDR technology – it will send Noteworthy Event and SPN Early Warning Event notifications to the Co-Managed XDR Service Team indicating that there is a certain breach, infection, or incident for a customer. Once the Service Team receives these notifications, an investigation will be started right away.

2. Assess Impact

- Perform endpoint/email assessment based on the malicious objects/IOCs (Indicator of Compromise) that have been identified.
- Perform cross-customer, cross-partner, and email/endpoint assessment.
- Performs IOC (Indicator of Compromise) assessment for critical advisory coming from different threat intel sources (ACSC, CISA, and Trend Micro Core Technology Team) to check if the network has already been affected.

3. Perform Root Cause Analysis

- Review/analyze logs from the Worry-Free Services Console.
- Perform root cause analysis to the noteworthy objects to determine other components/culprits of the infection.
- Remotely collect ATTK (Anti-Threat Toolkit) to identify malicious WMI, scheduled tasks, and autoruns.
- Collect suspicious/malicious objects for isolated testing.

4. Alert and Report to MSPs

- Send MDR alert (initial email notification) to the email address designated as the Incident Response Manager containing all the information gathered and the actions performed in the first hour.
- Provide timely updates regarding the noteworthy event being investigated.

III. Containment, Eradication, and Recovery

Isolate

Isolation focuses on containing the breach, so it does not spread and cause further damage to the organization.

The Co-Managed XDR Service Team can perform the following actions to contain the infection:

- Isolate endpoints to prevent lateral movements or further infection to other machines.
- Block noteworthy objects such as files and URLs to prevent execution.
- Quarantine malicious emails.
- Add malicious/suspicious object to User-Defined Suspicious Objects List.
- Terminate malicious processes

Eradicate

Once the issue has been contained, the Co-Managed XDR Service Team can find and eliminate the root cause of the breach. This means all malware should be securely removed, systems should again be hardened and patched, and updates should be applied.

The Co-Managed XDR Service Team can perform the following actions to eradicate the infection:

- Create/update product patterns for undetected files, URLs, and emails.
  - VRS (for files and processes)
  - WRS (for IP, domains, and hostnames)
  - BM (for behavior and file-less attacks)
  - ERS (for emails)
- Create cleanup tool for malicious autoruns, WMI, and scheduled tasks to prevent reoccurrence of the infection.
- Provide recommendations for vulnerabilities that have been exploited in the incident.
- Escalate to Threat Taskforce (if manual removal and root cause investigation is needed).
- Let the MSP verify if the malicious/suspicious object is deleted on the affected machines of the environment.
- Make sure that all security agents are updated to the latest agent version and pattern.
- Provide recommendation to MSP to run Worry-Free Security Agent Manual/Aggressive Scan.

Recovery

This is the process of restoring and returning affected systems and devices back into your business environment.

The Co-Managed XDR Service Team can perform the following actions to recover from the infection:

Provide information about the importance of backup and restore procedures:

- Send MDR recovery steps to the MSP, for example:
  - Addressing customer network issues.
  - Configure product best practice configuration.
  - Customer credential password reset.
  - System modification/ third-party Software/ OS patching.
  - Restore isolated endpoints.

Provide detailed incident report to the MSP. The report will include the following recommendations and reminders:

- To restore from backup in case of unrecoverable files (i.e. ransomware case).
- Ensuring that users have the minimum level of access required to accomplish their duties.
- Be wary of unknown URLs, embedded links and ads, attachments, and emails from unknown senders, especially with redundant requests for information, urgency, or insistence on immediate action.

Keep software updated:

- Software vendors regularly provide patches and updates to close whatever new vulnerabilities show up. As a best practice, validate and install all new software patches.
- Implement routine maintenance to ensure all software is current and check for signs of malware in log reports.

Educate users to prevent future attacks:

- Build awareness of common malware attacks.
- Keep users up to date on basic cybersecurity trends and best practices.
- Teach users how to recognize credible sites and what to do if they stumble onto a suspicious one.
- Encourage users to report unusual system behavior.
- Advise users to only join secure networks and to use VPNs when working outside the office.
- Double-check websites before logging in or signing up with sensitive information as these can be used against the organization with social engineering techniques, luring victims even after an initial attack.

Advise all users to follow email security best practices:

- Check for mismatched URLs. While an embedded URL might seem perfectly valid, hovering above it might show a different web address. In fact, users should avoid clicking links in emails unless they are certain that it is a legitimate link.
- Refrain from saving usernames and passwords on any browser.
- Users should always take the context of an email or message into account. For example, most online accounts do away with viewable member numbers, so users should be wary if they receive emails containing a "member number" for services that generally don't use them.

IV. Post-incident Activity

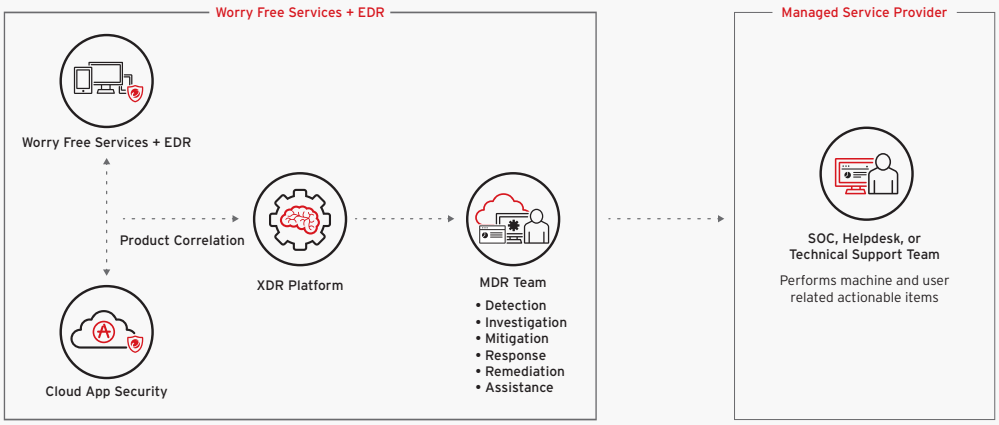
Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what have been learned from the data breach. This is where the team will analyze and document everything about the breach. Determine what worked well in the response plan, and where there were gaps that can be improved. Lessons learned from both mock and real events will help strengthen your systems against future attacks.

The Co-Managed XDR Service Team will:

- Work with backend developers to create and enhance noteworthy event rules for better detection of infections.
- Conduct bi-weekly "lessons learned" discussion with the team to talk about the errors in the previous cases and room for improvements.

Co-Working Model

This section will illustrate the co-working model between Trend's team and the Managed Service Provider



Co-Managed XDR Team

These are the actions that will be done by the MDR team:

- Detection
- Investigation
- Mitigation
- Response
- Remediation assistance

Managed Service Provider (MSP)

These involve SOC, helpdesk, or the technical support team on the MSP side.

Here are the actions required:

During Investigation:

- Manual upload of the suspicious file and email if MDR team failed to remotely collect it.
- Confirmation of the existence of the suspicious file.
- Verification on the integrity of the software involved.

After Investigation:

- Addressing customer network issues.
- Performing system modification, third-party software, and operating system patching.
- Initiating Worry-Free Security Agent Manual/Aggressive Scan.
- Run clean-up tool on the machine/s.
- Updating the Worry-Free Security Agent.
- Product configuration for best practice.
- Performing customer password reset.
- Provide end-customer advisory for the Incident.