

IT MANAGERS REGION 9 SEMINAR

Day 1 - Session 4

Trend Micro Presentation: Managed Detection & Response (MDR)

Presenters: Mark Ponte & Matt Chapman

Trend Micro

Tuesday, September 22, 2026

Session focus	MDR, EDR/XDR, telemetry, threat hunting, Chapter 13 exposure, Vision One, cyber-risk exposure management, security maturity, playbooks, lateral movement and incident-response considerations.
Document style	Detailed organized seminar notes. Discussion is consolidated by subject rather than reproduced as a running transcript.

Key Takeaways

- MDR was presented as 24x7 security expertise that augments the local IT team rather than merely another alerting product.
- The central technical theme was correlation: endpoint, network, email, identity and cloud data become much more useful when viewed together.
- The presentation repeatedly connected detection to response - tracing the entry path, containing the endpoint, identifying lateral movement and correcting the original failure point.

1. Trend Micro Background and Vulnerability Research

The presenters began by explaining Trend Micro's role as a cybersecurity company and its focus on enterprise security. They emphasized vulnerability research as part of the company's security model: researchers identify vulnerabilities, coordinate disclosure with the affected vendor and build protections before or while the vendor prepares its own patch.

The point for trustee offices was that endpoint/network protection can sometimes recognize exploitation behavior before every affected system has completed its normal patch cycle. This does not replace patching; it adds another layer during the period between discovery and complete remediation.

2. The Operational Problem MDR Is Intended to Solve

Small IT teams may own firewalls, endpoints and security tools but still lack someone continuously watching the environment. MDR was presented as a 24x7 service that adds security analysts as an extension of the customer's team.

The customer does not necessarily surrender control. Instead, the provider watches telemetry, investigates suspicious behavior, hunts for threats and can help contain incidents while the local IT manager continues handling the many other responsibilities of a trustee office.

3. Telemetry: Turning Device Data into an Attack Story

Telemetry was defined as security data collected from endpoints, firewalls, network devices, identity systems, email and cloud services. A single alert may be ambiguous, but multiple telemetry sources can be correlated to reconstruct what an attacker did.

The presenters repeatedly returned to the idea of following breadcrumbs. If malware appears on an endpoint, the investigation should not stop with cleaning that endpoint. Analysts want to know whether it arrived through email, whether the user account was compromised, whether the attacker moved laterally and whether the same indicators exist elsewhere.

4. EDR, XDR, MSS and MDR

EDR focuses on endpoint detection and response. XDR extends that concept by correlating data beyond the endpoint - for example, network, email and identity telemetry. The presenters noted that vendors do not always use the XDR label consistently.

An MSS/MSSP can function more like an outsourced security operation. MDR was described as a managed detection-and-response relationship in which the service works with the customer, provides continuous monitoring and human expertise, and supports investigation and containment.

The distinction matters when comparing vendors because two products can both use the word 'managed' while offering very different levels of human investigation, authority to respond and access to the underlying evidence.

5. Threat Actors and Why Chapter 13 Data Is Valuable

The presenters described a spectrum of threat actors ranging from less-skilled individuals using purchased tools to organized criminal groups and government-backed actors. The availability of malware, access brokers and ransomware services lowers the skill threshold required to launch attacks.

Chapter 13 environments hold information that attackers can monetize: personally identifiable information, financial information and privileged communications. The presentation's message was that attackers often choose the easiest valuable target rather than the most famous organization.

Compromise can also arrive indirectly. A debtor, creditor, attorney or other party may have a compromised mailbox, allowing an attacker to send a convincing message from a legitimate account into the trustee office.

6. Vision One and the Security Data Layer

Trend Micro's Vision One platform was presented as the place where the MDR team can see and correlate telemetry. The architecture is intended to work with a mixture of existing customer technologies rather than requiring every security component to be replaced.

The presenters discussed data sources that include endpoints, networks, email, identities, cloud services and applications. Bringing those sources together is what allows an analyst to see a sequence rather than a collection of unrelated alerts.

7. Cyber-Risk Exposure Management

The session introduced cyber-risk exposure management as a way to summarize current risk across assets, endpoints, cloud resources and users. The concept was compared to a speedometer: the objective is to show how the organization's risk changes as vulnerabilities, assets and user behavior change.

User behavior was part of the picture. People who repeatedly click phishing links can be identified for additional training, and exposure data can help prioritize where limited IT/security time should be spent.

8. Security Maturity, SIEM/SOAR Concepts and Playbooks

The presenters described security maturity as a progression from isolated tools toward centralized logs, analytics, automated workflows and continuous monitoring. Traditional syslog collection was discussed as an older form of centralization, while more mature environments add correlation and response automation.

A playbook defines what should happen when a known condition occurs. For example, if malware is confirmed on an endpoint, the response can automatically isolate that endpoint from normal network communication while preserving its ability to communicate with the security platform.

The important idea is speed and consistency: the system can contain a known threat immediately while analysts determine how it arrived and what else it touched.

9. Email, AI-Improved Phishing and Lateral Movement

Email was identified as a leading attack vector. The presenters contrasted older phishing messages - often easy to recognize because of poor language - with AI-assisted messages that can be polished and convincing.

Once a user clicks and the attacker gains a foothold, the attacker may move laterally through the environment, collect information, compromise identities and seek higher privileges. An administrator account is particularly valuable because it can turn a single-user compromise into a broader control problem.

Cross-layer telemetry helps reconstruct that movement: endpoint evidence can be connected to the email that delivered the payload, the network path it used and the identity activity that followed.

10. Perimeter Security Is Only One Layer

The discussion made clear that a firewall remains important but cannot be treated as the entire security program. Any public service requires some permitted traffic, and a vulnerability behind an allowed port can still be exploited.

Intrusion-prevention and other inspection features can add protection but also consume firewall resources. The larger architecture therefore needs endpoint controls, identity protection, monitoring, logging and response capability in addition to perimeter filtering.

11. MDR Service and Incident Response Considerations

The group discussed what happens when a real incident occurs, not just how alerts are generated. A useful MDR relationship must define who is monitoring, how the customer is contacted, what the provider can contain automatically, what evidence is retained and how incident-response resources are engaged.

The presenters indicated that their service can work alongside other partners rather than requiring the trustee office to abandon existing relationships. That is important for offices that already rely on STACS or another provider for parts of incident response.

12. Questions Raised When Comparing MDR Providers

Huntress and other MDR providers came up in discussion. Rather than reducing the comparison to a product-name contest, the session highlighted practical dimensions: breadth of telemetry, analyst coverage, global threat intelligence, response authority, integration with existing tools, escalation process and the ability to get experienced help during an actual event.

For a small office, the service model may matter as much as the underlying endpoint product because the core problem is not simply detecting an alert; it is having qualified people available to interpret and act on it.