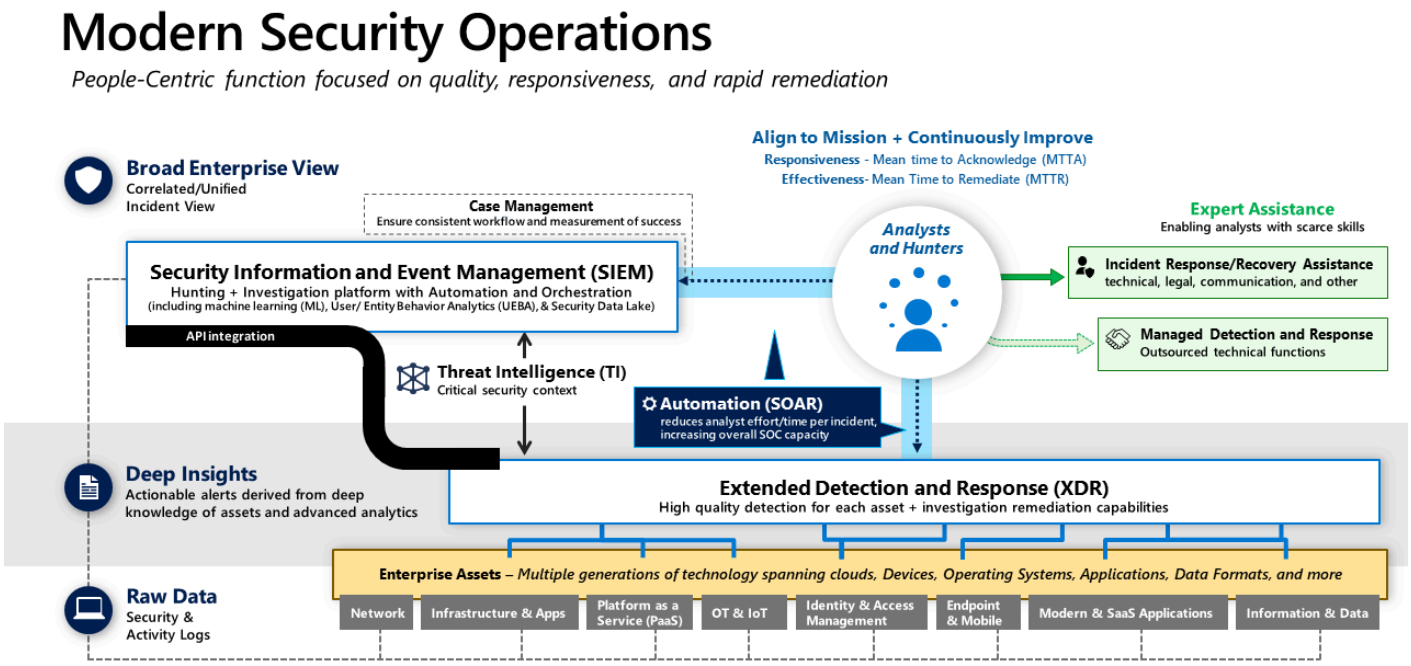
Microsoft Defender XDR in a Security Operations Center (SOC)

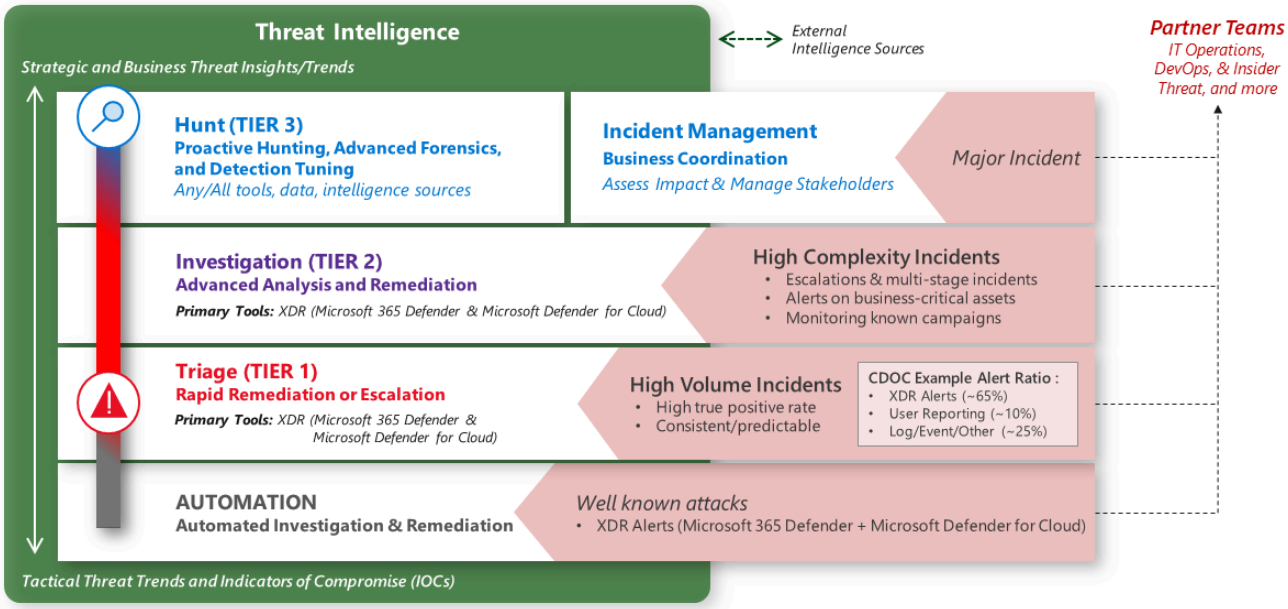


- *Overview of how Microsoft Defender XDR and Microsoft Sentinel are integrated in a Modern (SOC).*

Security Operations Model - Functions and Tools

The structure of security operations involves several distinct functions, with responsibilities varying based on **factors like organization size.** Each function or team has a primary focus area and collaborates closely with others for effectiveness. The diagram illustrates the complete model **with fully staffed teams.** In smaller organizations, these functions may be consolidated into a single role or team, managed by IT Operations for technical roles, or handled temporarily by leadership or delegates for incident management.

Security Operations Model – Functions and Tools



Triage and Automation

In addressing reactive alerts, our approach initiates with:

- **Automation:** Swift resolution of well-known incident types using near real-time automated processes. This pertains to clearly defined attacks that the organization has encountered frequently.

- Triage (Tier 1): Triage analysts concentrate on promptly resolving a **high volume** of recognized incident types that demand **quick human judgment**. They are responsible for approving automated remediation workflows and identifying anomalies or noteworthy elements that may require escalation or consultation with investigation (Tier 2) teams.

Key Insights for Triage and Automation:

- **90% True Positive:** Establish a quality standard of 90% true positive for alert feeds requiring analyst response to avoid excessive false alarms.

- **Alert Ratio:** Microsoft's experience in the Cyber Defense Operations Center indicates that XDR alerts yield most high-quality alerts, complemented by user-reported issues, log-query-based alerts, and others.

- **Automation Empowerment:** Automation significantly aids triage teams by empowering analysts and reducing the manual effort. For instance, it automates investigation steps and seeks human input before approving automated remediation sequences.

- **Tool Integration:** Microsoft Defender XDR integrates various XDR tools into a single console for endpoint, email, identity, and more. This integration enhances analysts' efficiency in swiftly identifying and mitigating phishing emails, malware, and compromised accounts.

- **Focused Expertise:** Due to the diverse nature of technologies and scenarios, these teams concentrate on specific technical areas or scenarios, often prioritizing user productivity, such as email, endpoint AV alerts, and initial response to user reports.

Investigation and Incident Management (Tier 2)

This team acts as the escalation point for issues from Triage (Tier 1) and directly monitors alerts indicating a **more sophisticated attacker**. They focus on behavioral alerts, **special case alerts** related to business-critical assets, and ongoing attack campaigns. Proactively, the team periodically reviews the Triage team alert queue and **engages in proactive hunting using XDR tools during downtime.**

They conduct **deeper investigation**s into a lower volume of complex attacks, often multi-stage attacks orchestrated by human operators. The team also pilots new or unfamiliar alert types to document processes for the Triage team and automation, including alerts generated by Microsoft Defender for Cloud on cloud-hosted apps, VMs, containers, Kubernetes, SQL databases, etc.

Incident Management – This team handles the non-technical aspects of managing incidents, coordinating with other teams such as communications, legal, leadership, and other business stakeholders.

Hunt and Incident Management (Tier 3)

This multi-disciplinary team focuses on identifying attackers who may have **evaded reactive detections and managing major business-impacting event**s.

Hunt – The team **proactively** searches for undetected threats, assists with escalations, and conducts **advanced forensics** for reactive investigations. Operating in a hypothesis-driven model, they also connect with red/purple teams in the security operations realm.

How It Comes Together

To illustrate the process, let's follow a common incident lifecycle:

1. A Triage (Tier 1) analyst **claims** a malware alert, investigates using the **Microsoft Defender XDR console.**
2. If the case requires advanced remediation, Triage escalates it to the Investigation analyst (Tier 2), who leads the investigation. The Triage team may stay involved for learning purposes (using **Microsoft Sentinel** or **another SIEM** for broader context).
3. Investigation verifies conclusions and proceeds with remediation, closing the case.
4. Later, Hunt (Tier 3) might review closed incidents to scan for commonalities or anomalies, looking for potential auto remediation, common root causes, or process/tool/alert improvements.

For example, Tier 3 may identify a tech scam that warrants a higher priority alert due to the scammers obtaining admin-level access on the endpoint.

Threat Intelligence

Threat Intelligence teams provide context and insights to support all other functions, using a Threat Intelligence Platform (TIP) in larger organizations. This includes reactive **technical research** for active incidents, **proactive** technical research into attacker groups, **attack trends**, **high-profile attacks**, emerging techniques, and strategic analysis to inform business and technical processes and priorities.