

Extended Detection and Response with Microsoft 365 Defender

In the previous chapter, the focus was on Microsoft Defender Vulnerability Management and Secure Score. This chapter will focus on **eXtended detection and response (XDR)** with **Microsoft 365 Defender (M365D)**, what it is, and what separates it from other security tools such as **Endpoint Detection and Response (EDR)**, **Network Detection and Response (NDR)**, and **Security Information and Event Management (SIEM)**.

By following this chapter, you will gain knowledge on how to operate M365D as an XDR for use in real-world scenarios when your organization comes under attack from a malicious actor.

We will cover these main topics throughout the chapter:

- Introducing XDR
- How M365D works as an XDR
- Understanding incident response and management

How M365D differs from a traditional SIEM solution

Introducing XDR

XDR is a compilation of tools and technologies that work together to monitor and mitigate cyber security threats in an environment. Much like SIEM, it relies heavily on collecting data from multiple sources such as endpoints, servers, cloud workloads, and collaboration services. An EDR

solution only monitors the endpoints onboarded to that solution, which will leave blind spots in comparison to an XDR. An XDR solution will then analyze and correlate said data to provide visibility and context and help reveal other threats using correlated data to help you identify in a more granular way what happened, which devices and users were involved in the incident, and whether there are any other cases that match that correlation throughout your environment.

So basically, an XDR is a security tool that helps you gain insights into your current environment and helps you mitigate threats found within it. Think of it as the next step in security, unifying all security services in one place.

M365D is an XDR based on this definition because, as we have covered in this book, all the security services **Microsoft Defender for Endpoint (MDE)**, **Microsoft Defender for Identity (MDI)**, **Microsoft Defender for Cloud Apps (MDA)**, and **Microsoft Defender for Office 365 (MDO)** correlate the alert data gathered from any of these services and provides you with detailed insights into what has happened.

Now that we know what an XDR is, let us look at how to use M365D as that XDR.

How M365D works as an XDR

M365D automatically collects, correlates, and analyzes alert and threat data from across your endpoints onboarded to MDE, your emails from MDO, your applications from MDA, and your identities from Azure **Active Directory (AD)** Identity Protection and MDI. M365D uses **artificial intelligence (AI)** and automation to help you stop attacks automatically and remediate affected entities into a compliant state once more.

Unlike the EDR part of M365D (Defender for Endpoint), which is a post-breach security service, the XDR service is a unified pre- and post-breach security service.

The following diagram illustrates an ongoing attack, starting with a phishing email arriving in an unsuspecting user's mailbox. The user unknowingly opens the attachment, installing malware on the user's endpoint, which is then used to move laterally within the environment gaining higher privileges and ultimately exfiltrating data:



Figure 18.1 – The Defender services acting against an attack

As described in the preceding diagram, the following security services help stop this attack:

- **Exchange Online Protection (EOP):** Part of MDO, this can detect phishing emails and make use of mail flow rules to ensure that the malicious email never reaches the intended recipient
- **MDO:** Uses safe attachments to test the attachment and determine whether it is harmful or not
- **MDE:** Detects the malware if it is missed by EOP or MDO by always monitoring the device
- **MDI:** Detects sudden account changes, such as escalation of privileges or lateral movements
- **MDA:** Detects unusual user behavior such as impossible travel or activity from an infrequent country

The attack shown in *Figure 18.1* would not be successful if the security services in M365D were configured as we have talked about in this book so far since they would work together to stop the attack in near real time.

M365D automatically correlates the relevant data for the attack outlined using AI and takes the actions it sees fit to ensure the threat is mitigated. The drawback of relying heavily on M365D taking these decisions for you

is just that. You lack control over what mitigating actions are implemented and why.

Based on that assumption, let us look at what an incident is and subsequently how to respond to said incident, kicking the threat actor out of here!

Understanding incident response and management

An **incident** in M365D is a collection of correlated alerts and data that together makes up the story of an attack. As mentioned throughout this book, Microsoft 365 services and applications generate alerts when they detect suspicious or malicious activity occurring. While individual alerts do provide valuable information on a completed or active attack, a modern attack often relies on using various techniques against different types of entities. The result is several alerts for several entities in your environment.

Piecing this information together manually to gain the necessary insights can be both time-consuming and challenging, which is why M365D aggregates the alerts and the associated information into an incident, as illustrated in the following diagram:

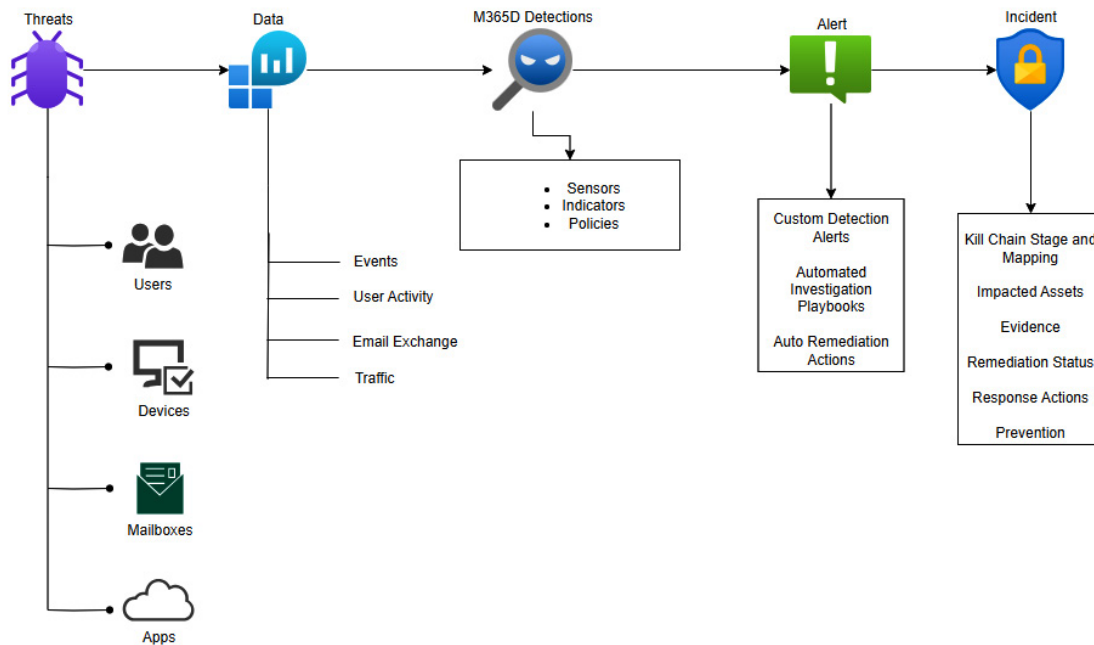


Figure 18.2 – The correlation of entities, associated information, and alerts with an incident

By grouping the alerts into an incident, it provides you with a detailed view of the attack allowing you to answer the following questions:

- Where did the attack start?
- Which **tactics, techniques, and procedures (TTPs)** were used?
- How far did the attack go into the environment?
- What is the scope of the attack, and how many devices, users, and mailboxes were affected?

In M365D, an incident might look something like the following:

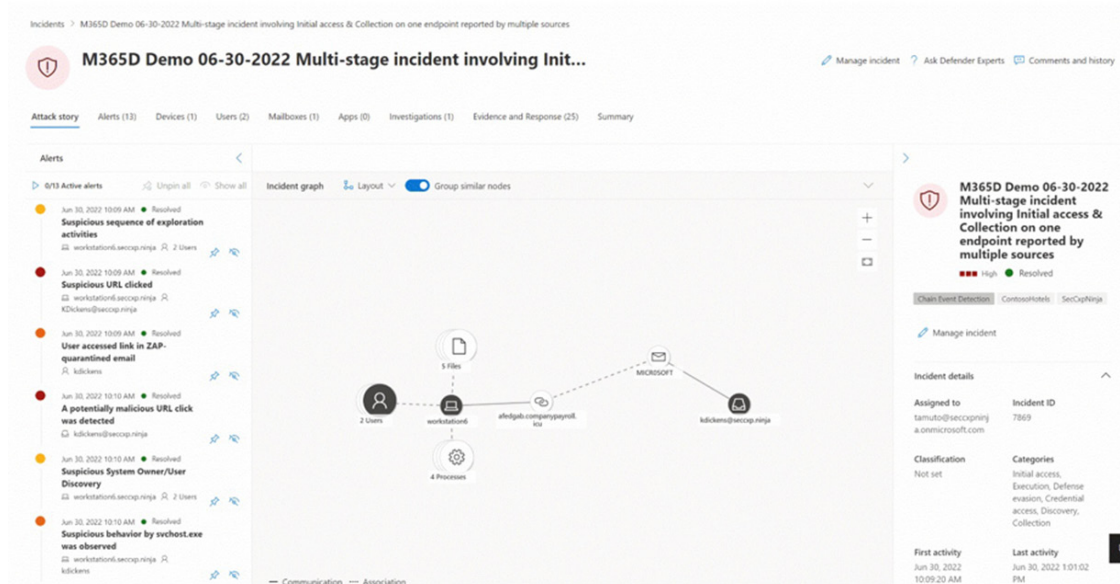


Figure 18.3 – An example incident showing the attack story in M365D

As we have covered, an incident in M365D consists of multiple alerts grouped into one incident to better identify entities affected and to clarify what is or has happened.

Now, let us move on to how to respond to an incident using M365D.

Responding to incidents in M365D

Incidents are inevitable in any IT environment, no matter how well-designed or well-managed it may be. When an incident occurs in M365D, it is important to respond quickly and effectively to minimize the impact and prevent any further damage. This chapter provides an overview of the incident response process and outlines the steps you should take to respond to incidents.

This process in M365D consists of the following stages:

- **Detection:** The first stage of incident response is detection, where an incident is identified through various means, such as alerts, notifications, or user reports. To detect incidents in M365D, you can set up alerts for various security events such as malware detections, suspicious login attempts, or data exfiltration. This can be done by adding

custom alert policies for the various workloads, either via the portals themselves or via Custom Detections based on **Kusto Query Language (KQL)** queries you specify. Constructing these queries will be covered later in this book in [Chapter 19](#).

- **Triage:** Once an incident has been detected, it is important to triage it to determine the severity and impact of the incident. This involves collecting information about the incident, analyzing it, and assigning it a priority level. When an alert is triggered, or a potential incident is detected, it will appear in the incident queue in the M365D portal. To access the incident queue, navigate to the **Incidents** section. From here, you can view all open incidents and filter them by severity, category, or status:

Incidents Create a notification rule

Most recent incidents and alerts

1-8 < > 6 months Choose columns 30 items per page Filters

✓	Incident name	Tags	Severity	Investigation state	Categories
<input checked="" type="checkbox"/>	> Multi-stage incident involving Initial access & Exfiltration on one endpoint...	asdf tag test02	High	2 investigation states	Initial access, Execution,
>	Multi-stage incident involving Initial access & Exfiltration on multiple end...	asdf tag test02 IT Team +3	High	2 investigation states	Initial access, Execution,
>	Multi-stage incident involving Initial access & Exfiltration on one endpoint...	ar test01 asdf tag test02	High	4 investigation states	Initial access, Execution,
>	Multi-stage incident on one endpoint reported by multiple sources	asdf tag test02	Medium	2 investigation states	Persistence, Suspicious

Figure 18.4 – The Incidents queue in M365D

You can also assign incidents to specific users or teams for triage and investigation:

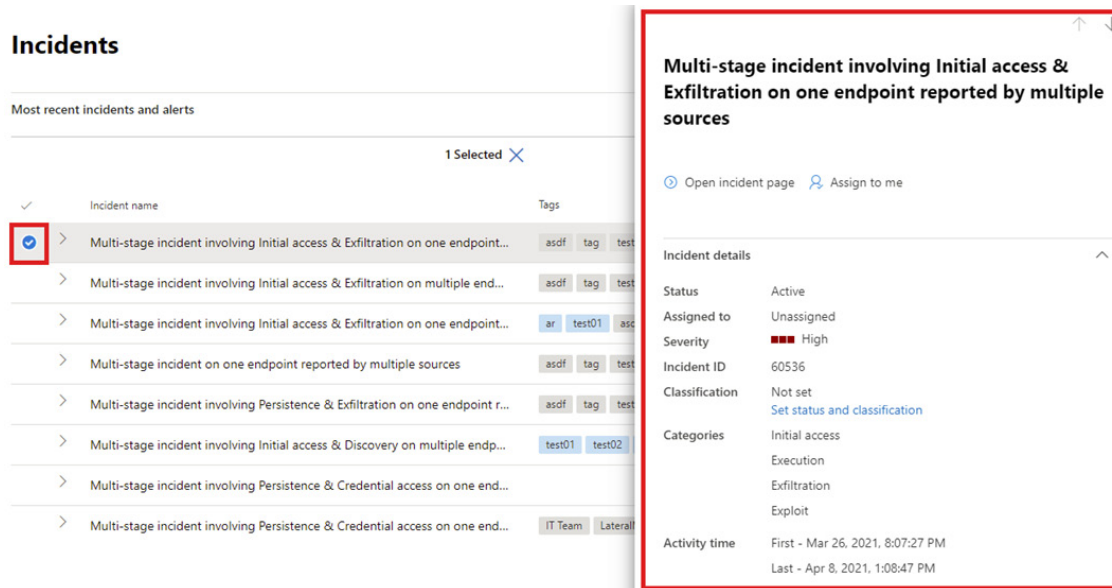


Figure 18.5 – The incident summary page for the selected incident

- Containment:** The next stage is containment, where the incident is isolated to prevent it from spreading further. This may involve taking actions such as quarantining affected systems or blocking malicious IP addresses. These actions can be categorized as follows:
 - Automated actions:** M365D includes several automated actions that can be triggered in response to security events. For example, you can configure automatic remediation actions such as blocking or quarantining affected devices or users or resetting compromised credentials. This will also be covered in [Chapter 19](#).
 - Manual actions:** In some cases, manual intervention may be required to contain an incident. For example, you may need to disable a compromised user account, isolate an affected device, or block a suspicious IP address. To perform manual actions, we can open an active incident and perform actions directly on the affected devices or users from the M365D portal, as showcased in the following screenshot, and explained in more depth in the section *Device and User Respond Actions*:

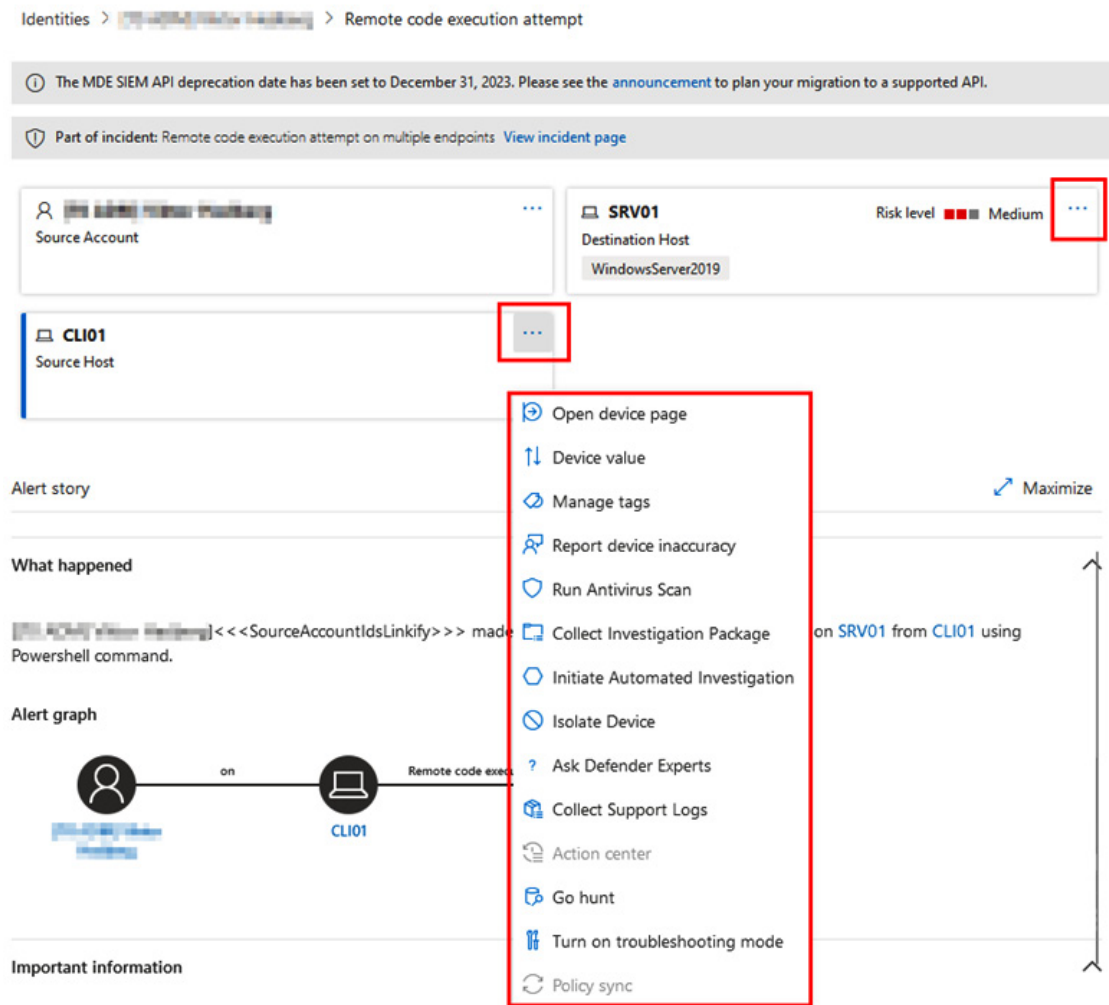


Figure 18.6 – Device actions presented directly from an incident in the M365D portal

- **Investigation:** With the incident contained, the next step is to investigate the incident to determine the root cause, scope, and impact of the incident. This involves analyzing logs and other data to identify the source of the incident and any affected systems or users. In the context of an attack, the **Alert** page and incident graph are two key elements that provide valuable information.
 - The incident alert page contains several sections, including **Attack story**, which describes what happened, actions taken, and related events. The alert properties can be found on the right-hand side of the page and include details such as the state, description, and other pertinent information. It's important to note that not all alerts will contain every subsection listed in the alert story section.

- The **Incident graph** section, on the other hand, provides a visual representation of the attack's full scope. It illustrates how the attack spread through the network over time, its point of origin, and the extent of the attacker's reach. Suspicious entities that are part of the attack are linked to related assets such as users, devices, and mailboxes:

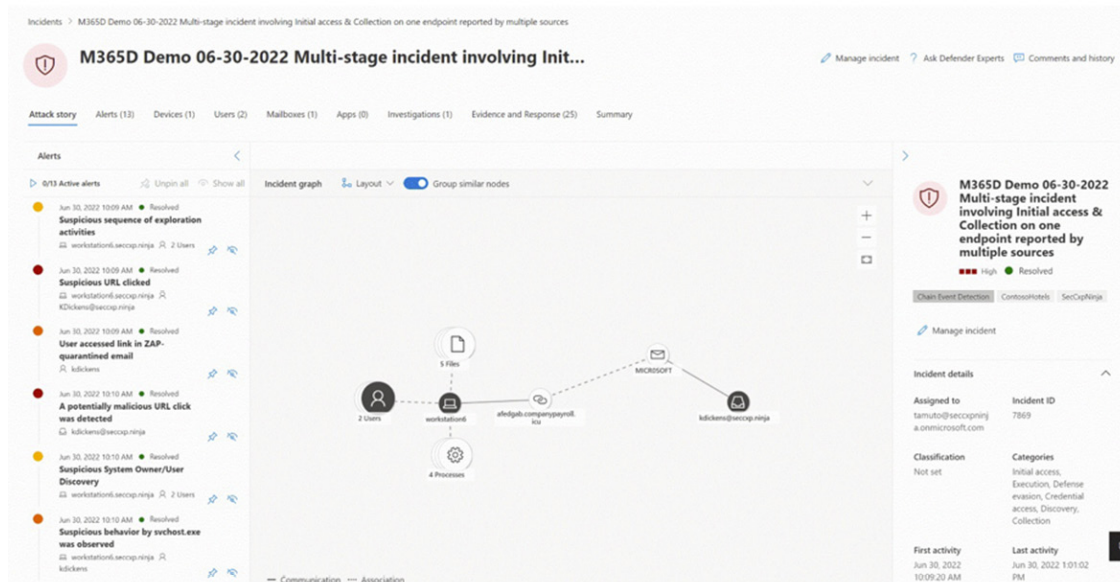


Figure 18.7 – The Attack story tab on an active incident allows you to quickly review the full story of the attack

- **Remediation:** Once the investigation is complete, the incident can be remediated by taking actions such as applying patches, removing malware, or resetting compromised accounts.

This can partly be done via the M365D portal, but for the bulk of these actions, you need to perform them within the respective platform.

Intune/Configuration Manager/Windows Server Update Services for applying patches and AD/Azure AD for password resets.

- **Recovery:** The final stage of incident response is recovery, where systems and data are restored to their pre-incident state. This involves verifying that all systems are functioning properly and that any necessary backups are in place.

To wrap up the incident response part of this chapter, I'd like to add that Microsoft has compiled several incident response playbooks for different scenarios on the Microsoft Learn website

(<https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks?view=o365-worldwide>).

These playbooks offer insights from the Microsoft **Detection and Response Team (DART)** on how to act under certain circumstances.

To summarize, incident response in M365D can be almost fully managed via the portal. Up next, let us look at how we can manage the **automated investigation and response (AIR)** feature of M365D.

Managing AIR

AIR is a feature in M365D that helps security teams automatically detect, investigate, and remediate security incidents. It is designed to enable a proactive and efficient response to threats by automating the security operations process. This feature can help security teams to identify and mitigate security incidents faster and more accurately.

The AIR feature consists of several components, including:

- **Automated investigation and remediation:** This component enables the automatic investigation and remediation of security incidents. It is based on predefined playbooks that are designed to automate the incident response process. These playbooks can be customized to meet the specific needs of an organization.
- **Automated incident creation:** This component automatically creates incidents based on the alerts generated by M365D. The system can automatically triage and prioritize alerts and create incidents based on the severity and criticality of the alert.
- **Automated response:** This component enables automatic response to security incidents. The system can automatically quarantine or block malicious files, devices, or users based on predefined policies. It can

also trigger other actions, such as sending notifications, creating tickets, or generating reports.

- **Automated hunting:** This component uses your custom detections in M365D to automatically hunt for potential security threats in the organization's environment. It can identify suspicious activities or anomalies that might indicate a security incident.

The benefits of this feature in M365D include the following:

- **Faster AIR:** AIR can detect and respond to incidents faster than traditional manual methods, reducing the impact of security incidents
- **Consistency and accuracy:** This feature can ensure that incidents are handled consistently and accurately, minimizing the risk of human error
- **Improved efficiency:** It can reduce the workload of security teams, enabling them to focus on higher-value tasks
- **Customizability:** It can be customized to meet the specific needs of an organization, enabling it to tailor its security operations to its unique environment

Overall, AIR is a powerful feature in M365D that can help organizations to improve their security posture by automating the incident response process. It can help security teams to detect and respond to incidents faster and more accurately, reducing the impact of security incidents in the organization.

To manage this feature, we stay in the portal, navigating to **Settings** | **Endpoints** | **Advanced features**:

Endpoints

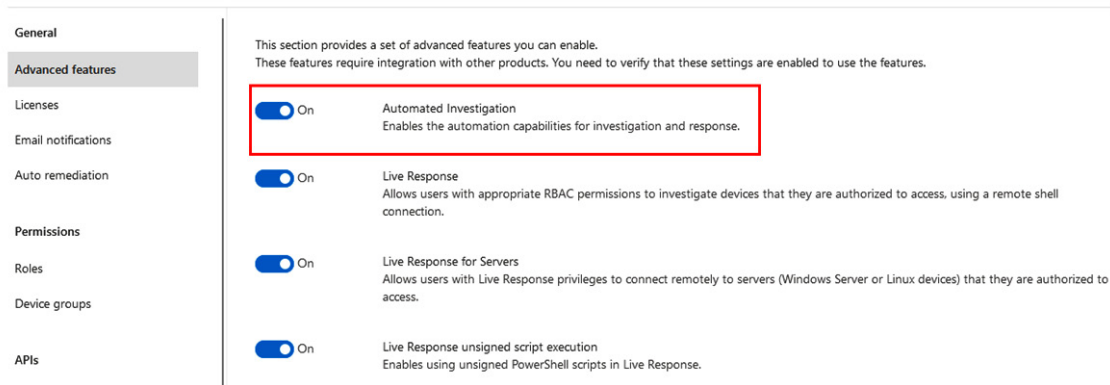


Figure 18.8 – The toggle to enable AIR capabilities in M365D

This is an *On/Off* feature that cannot be scoped to be enabled for a subset of users or devices. It's an all-or-nothing kind of setting.

When working with device groups in MDE, we can specify the level of automation for each device group. MDE leverages the power of AIR to enhance its incident response capabilities.

To configure different levels of automated investigation and response in M365D, perform the following actions:

1. In MDE, create a device group by selecting **Device groups** and clicking **+ Add device group**:

Endpoints

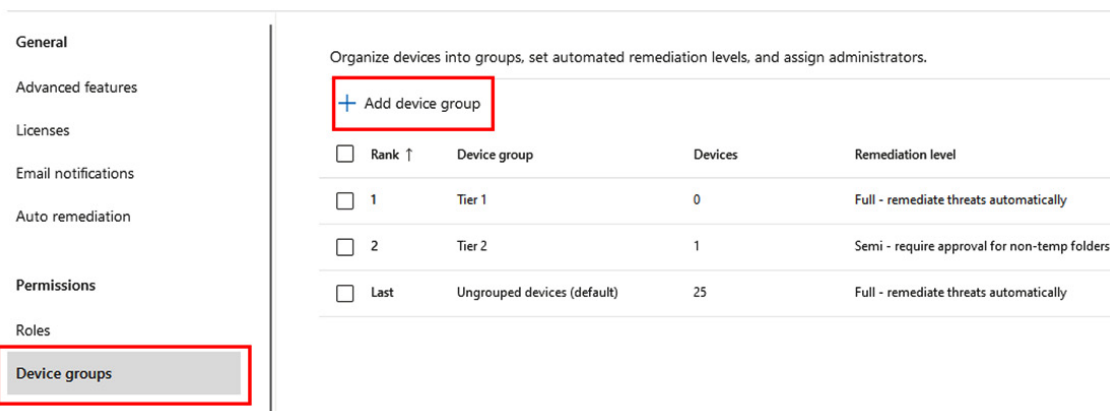


Figure 18.9 – Creating a new device group

2. On the **General** tab of the new device group, add a name and select one of the automation levels for this device group that were discussed earlier in this section:

General

Provide a name and a description for this notification rule to make it easier to identify and manage.

The screenshot shows the 'General' tab configuration for a new device group. The 'Device group name' field is highlighted with a red box and contains the text 'Mastering Microsoft 365 Defender'. Below it, the 'Remediation level' dropdown menu is also highlighted with a red box. The dropdown is open, showing five options: 'No automated response', 'Semi - require approval for all folders', 'Semi - require approval for non-temp folders', 'Semi - require approval for core folders', and 'Full - remediate threats automatically'. The 'Full' option is selected and highlighted with a grey background.

Figure 18.10 – Selecting the automation level for a device group

DIFFERENT TYPES OF REMEDIATION LEVEL

For a full reference guide on the different remediation levels, Microsoft's official documentation does a great job of explaining things:

learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels

3. Once the automation level has been assigned, add the devices to your device group by filtering on **Name**, **Domain**, **Tag**, and **OS**:

Devices

Specify the matching rule that determines which devices belong to this group.

4 items


And/Or	Condition	Operator	Value
	Name	Starts with	<input type="text"/>
And	Domain	Starts with	<input type="text"/>
And	Tag	<input checked="" type="checkbox"/> Windows Server 2022 <input type="checkbox"/> Windows 11 <input type="checkbox"/> Windows 10 <input type="checkbox"/> Windows 8.1 <input type="checkbox"/> Windows 8 <input type="checkbox"/> Windows 7 <input checked="" type="checkbox"/> Windows Server 2019 <input checked="" type="checkbox"/> Windows Server 2016	<input type="text"/>
And	OS		Windows Server 2022, Wi... <input type="text"/>

Figure 18.11 – Filtering devices to belong to a device group based on server operating systems

- On the **Preview devices** tab, we can preview which devices onboarded to MDE will populate this device group:

Preview devices

Shows up to 10 devices. If a device in this group matches groups with a higher rank, it will show in the preview but will only be added to the group with the highest rank.

 Show preview

6 items







Device name
 \psdo001
 \labdc01
 \srv01
 \ca01
 \demotiering
 \host01

Figure 18.12 – The Preview devices page

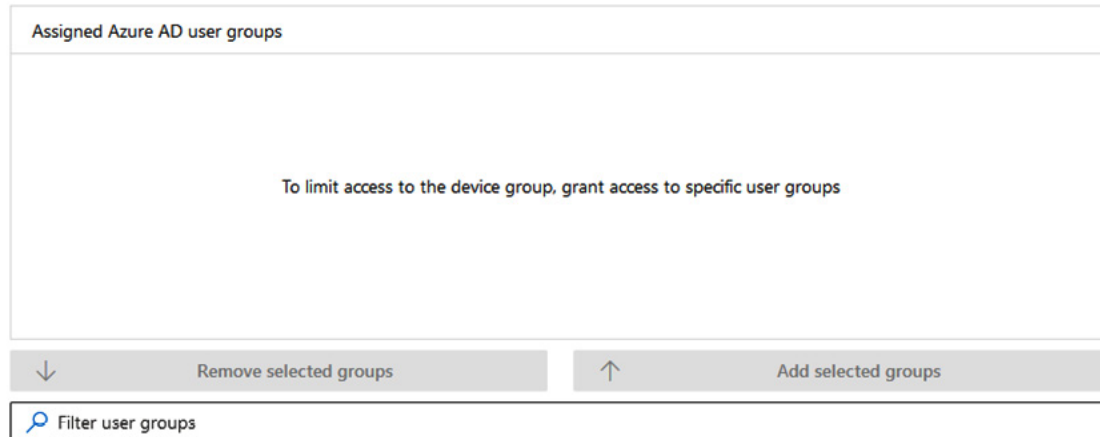
- On the last page, we can specify access provided that the tenant is enabled for **Role-Based Access Control (RBAC)**. If the tenant is not, we simply create the device groups after *step 4* in this list, and the settings

we have applied will follow suit. When configuring RBAC in M365D, it is imperative to remember to use role assignable groups, also known as **Privileged Access Groups (PAGs)**, as they only can be modified by the group owner, a global administrator, or a privileged role administrator:

User access

Access to devices in the group

Select the Azure AD user groups that should have access to this device group.



Assigned Azure AD user groups

To limit access to the device group, grant access to specific user groups

↓ Remove selected groups ↑ Add selected groups

Filter user groups

Figure 18.13 – Using RBAC in M365D

This concludes the section on how to configure the AIR feature; we will touch back on this in [Chapter 19](#), as the Custom Detections in M365D can perform similar tasks on an entity.

Up next, we will look at **automated attack disruption**.

Managing automated attack disruption

Automated attack disruption is a vital feature of M365D that helps contain attacks and minimize their impact on an organization's assets. This feature is different from other known protection methods, such as **blocking** based on a single indicator of compromise. Instead, it leverages the full breadth of the platform's XDR signal to act at the incident level, taking the entire attack into account.

Unlike many other XDR and SOAR solutions that allow users to create their own response actions, M365D's automatic attack disruption is built-

in and uses insights from security researchers and advanced AI models to counteract the complexities of advanced attacks. It considers the entire context of signals from different sources to determine compromised assets. You can also use Logic apps to perform automated responses.

Automatic attack disruption operates in three stages:

1. M365D's XDR ability correlates signals from many different sources into a single, high-confidence incident using insights from endpoints, identities, email, and collaboration tools, as well as **software-as-a-service (SaaS)** apps.
2. Assets controlled by the attacker and used to spread the attack are identified.
3. Relevant Microsoft Defender products take automatic response actions to contain the attack in real time by isolating affected assets.

By limiting a threat actor's progress early on, automatic attack disruption significantly reduces the overall impact of an attack. It helps to minimize associated costs and loss of productivity, making it a game-changing capability for organizations that rely on M365D to keep their assets secure.

A core part of automated attack disruption is the AIR feature in MDE, a topic we covered previously in this chapter. The only thing that can be done to exclude entities from AIR and Automated attack disruption is to lower the security posture of your environment and select the **No automated response** option for a subset of devices. For identity entities, we need to exclude them from this option by heading back to the portal and performing these steps:

1. Head to **Settings and Identities**.
2. There is a section called **Automated response exclusions** where we can add excluded users:

Microsoft Defender for Identity

The screenshot displays the Microsoft Defender for Identity console. On the left, a navigation pane lists various settings categories: General, Entity tags, Excluded entities, and Notifications. The 'General' section is expanded, showing options like Sensors, Directory services accounts, Manage action accounts, VPN, Health issues, Portal redirection, Advanced settings, and About. The 'Entity tags' section includes Sensitive, Honeytoken, and Exchange server. The 'Excluded entities' section is highlighted, with 'Automated response exclusions' selected and outlined in red. The 'Notifications' section includes Health issues notifications, Alert notifications, and Syslog notifications. The main content area is titled 'Exclude users from automated response actions' and features a '+ Exclude users' button (also outlined in red), a '↓ Export' button, and a table with columns for 'User' and 'Domain Name'. The table is currently empty, displaying 'No data available'.

Figure 18.14 – Automated response exclusions

IMPORTANT NOTE

It is not recommended to exclude either devices or users from the automation in M365D as it greatly diminishes the environment's security posture and your possibilities of staving off an attack.

This covers how to exclude users and devices from the automation inside M365D. To explore how you can perform manual response actions for devices and users, keep reading the next section.

Real-time response with device, file, and user actions

Earlier in this chapter, we explored responding to incidents. Let's now explore, in more depth, some of the actions we can perform in the Microsoft 365 Defender portal. We can break these down into three response action types: device, file, and user.

Device response actions

To respond to investigations, incidents, and threats, an administrator can invoke the following types of response actions to an onboarded device from the **Device** page or any reference to a device in the investigation and alert interfaces. Let's check out the full list before exploring the key ones in more detail:

- **Run Antivirus Scan**
- **Collect Investigation Package**
- **Restrict App Execution**
- **Initiate Automated Investigation**
- **Initiate Live Response Session**
- **Isolate Device**

There are others that are a bit more intuitive and, therefore, we'll skip over them (such as **Exclude** and **Report device inaccuracy**), and you can also expect more to be added over time.

Each OS has different device response capabilities, as the actions are implemented by that OS's MDE service, which varies from platform to platform. For example, it's intuitive that the response actions from Android and iOS are different from those for Windows and macOS. But, even on Windows, we have different capabilities: devices older than Windows Server 2012 R2 and Windows 10 (server and client, respectively), cannot perform device response, automatically or manually.

Now that you're aware of why we don't get complete feature parity across platforms, let's review the six key device response actions.

Run antivirus scan

This is available in both passive mode and active mode and does what it says on the tin. You will have the option to initiate a quick or full scan, with either option also updating the definitions first.

Collect investigation package

When you collect an investigation package, a request is submitted to the device, and after this is fulfilled, you will be able to download a ZIP file with forensic data such as CSVs of installed programs, processes, services, and Task Scheduler entries, lists of users and groups, files in temporary directories, and other useful data.

After you start the investigation package collection, the **Action center** popup will appear with the action pending. You can jump back to the Action center at any time to see a history or status of actions.

When the ZIP file is available, this changes **Status** to **Package collection package available**, and you can download it. This is depicted in *Figure 18.15*:

Action center

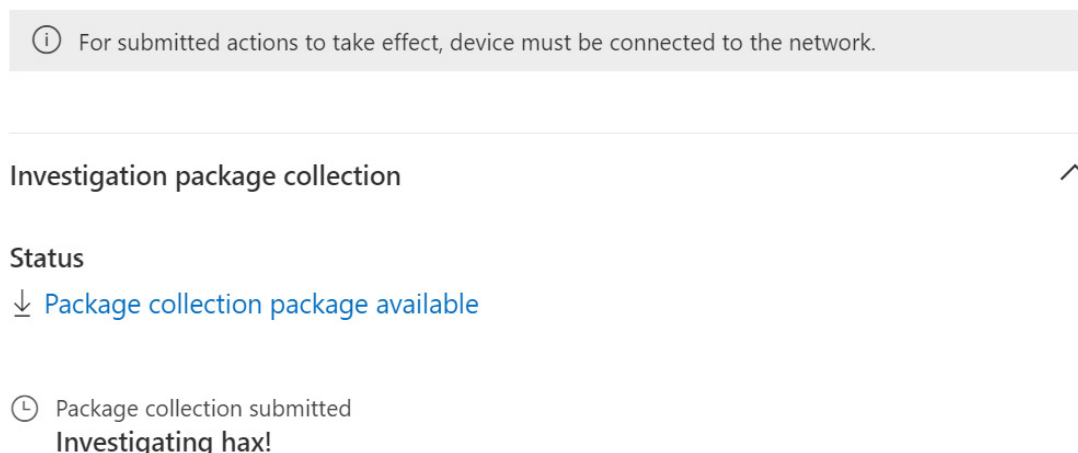


Figure 18.15 – Collecting an investigation package

Restrict app execution

This is available only for Windows 10+ and Windows Server 2019+, with app restriction using code integrity to only allow file execution if signed by Microsoft. This is useful if you suspect a device has been compromised and need to take immediate action. The end user is notified with a popup, and you can reverse the restriction by selecting the option again, as it transforms to **Remove app restrictions**.

Initiate automated investigation

Earlier in this chapter, you learned about automated investigations. This option invokes one manually if, for example, an alert or investigation did not automatically invoke one for a device of interest.

Initiate live response session

Live response is a remote shell capability that gives operators real-time response capabilities directly on the device. Using commands, live response lets you view information such as installed drivers (the **drivers** command), search for files (**fileinfo**), and show scheduled tasks (**scheduledtask**). Viewing or retrieving information commands are known as **basic commands**, and administrators can be limited to only these with RBAC.

You can also perform actions using **advanced commands**, which can also be delegated to specific roles only. For example, you can use the **Upload file to library** option, seen in *Figure 18.16*, to upload a PowerShell script that can then be executed using the **run** command:

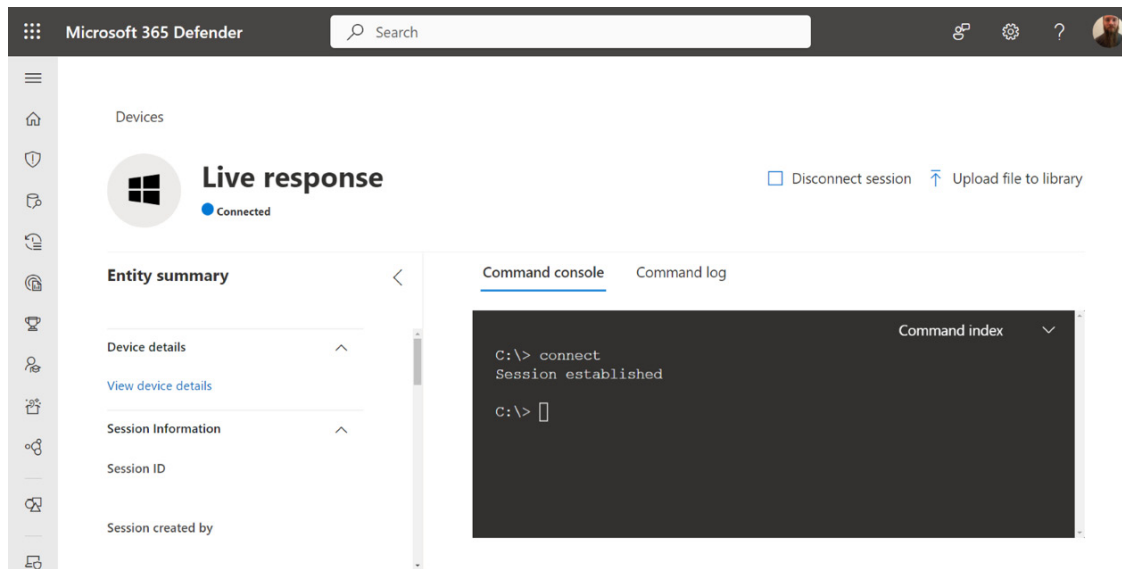


Figure 18.16 – Running live response

As you can imagine, the ability to immediately run PowerShell scripts gives you a near-infinite number of response capabilities, which may include invoking other security platforms. With great power comes great responsibility, so make sure your live response permissions are managed carefully, particularly on important devices such as domain controllers.

Other live response advanced commands include **remediate**, which can be executed against files, services, scheduled tasks, or startup items to stop, delete, or remove them; **isolate**, which you'll read more about shortly; and **putfile**, which lets you move other files from the library to the device.

At the time of publication, some device response actions for macOS and Linux can only be invoked using live response. For example, **run antivirus scan**, **isolate device**, and **collect investigation package** can't be chosen from the device page, only by using live response commands.

FULL LIVE RESPONSE REFERENCE

There are lots of live response commands, and their availability differs from platform to platform. Microsoft's documentation has an excellent reference: learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response.

Isolate device

This is a powerful response action but proceed with caution. When you isolate a device, it blocks network communications for everything other than MDE. This may include services you'd use to remediate threats, such as third-party protection platforms, Intune, or VPNs. You should be especially careful running this on Hyper-V hosts, as all VMs running on that server will be affected.

With these warnings out of the way, isolating devices is an effective way of containing threats. You'll slow down, if not entirely block, attack paths, lateral movement, and data exfiltration. On Windows 10, you can use selective isolation to exempt Outlook and Teams, so that you can still communicate with the user.

Just like with the restriction of app execution, you can undo device isolation, as the same button that enabled it transforms into **Release from isolation**.

That's the most significant device response actions covered, so let's check out file response capabilities.

File response actions

When files are discovered on devices or become relevant objects in alerts and investigations, they get a file page. You can find these pages either through the alert or investigation, or by searching for the file in the Microsoft 365 Defender portal's toolbar. You can search by hash or filename, as depicted in *Figure 18.17*:

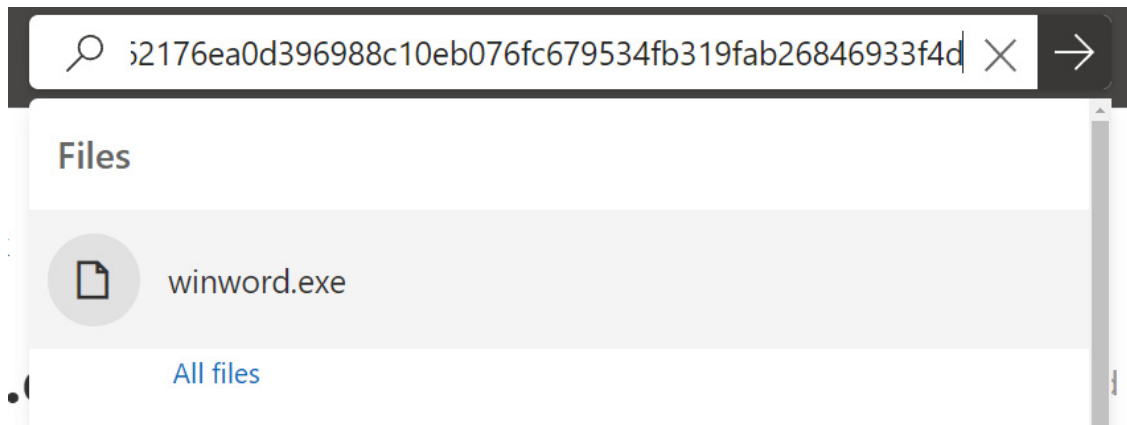


Figure 18.17 – Searching for a file based on the SHA256 reference

When you land on the file page, you can find out information such as related incidents, VirusTotal ratio, first/last seen dates, and prevalence (worldwide and just in your organization). This information is useful for ascertaining how risky the file might be. After reviewing the data, you'll be able to invoke the following actions:

- **Stop and quarantine**
- **Add indicator**
- **Download file**
- **Submit for deep analysis**

Let's have a look at each of these.

Stop and Quarantine

For Windows and Windows Server devices, you can use this to stop the file if already running, then send it to the quarantine. End users will be notified, and to get the file back from quarantine, you'd need to have access to the device itself, rather than a central quarantine.

Files signed by Microsoft or meeting certain trust criteria, such as signed and verified publishers, cannot be controlled using this action: you'll find the option grayed out.

Add Indicator

You learned about indicators in ***Chapter 5***. There, we explored indicators to exclude files. Using the option to add an indicator from the file page, you can quickly exclude or apply one of the following actions:

- **Audit**
- **Warn**
- **Block execution**
- **Block and remediate**

When you audit a file, you can optionally generate an alert, which makes this a useful option if you want to investigate but not do any kind of blocking. When you warn with a file, think of it like a block with override: the file is stopped from executing but users can override it. The difference between **Block execution** and **Block and remediate** is the former allows the file to remain on the device, just not allowed to run, whereas the latter removes it entirely.

Download file

If you need to retrieve a file for your own investigation, this response action provides it to you in a password-protected ZIP, where you choose the password. If you suspect the file is malicious, you should, of course, be cautious when opening it, ideally on an investigation-dedicated device.

File collection is dependent on sample submissions being enabled, which you'll have configured in the various onboarding chapters earlier in this book. If the file has never been uploaded to the MDE service, you will see **Collect file** instead of **Download file**. This means the service will reach out to the device to try and obtain it, which may or may not be successful depending on the status of the file and device (removed and/or offline).

Submit for deep analysis

Last but not least, the deep analysis feature for files is only available for files discovered on Windows devices. This capability *detonates* the file in

a cloud sandbox and looks for the results of running that file, rather than just the file's signatures. This is comparable to Safe Attachments in MDO.

Deep analysis can take some time. The portal advises up to three hours, which is also the timeout for collecting files it doesn't already have in the service. After the analysis finishes, you'll be able to dig into behaviors and observations.

Next up, we're going to check out the types of response actions available for users.

User response actions

Just like with devices and files, you'll end up on a user page either by searching for them or navigating through alerts and incidents. As well as risky information on the user page, you can invoke actions. The key ones are as follows:

- **Confirm user compromised**
- **Suspend user in AAD**
- **Suspend user in AD**
- **Force password reset**
- **Require user to sign in again**

For the actions that require on-premises interaction, such as **Suspend user in AD** and **Force password reset**, the action account you configured in [*Chapter 12*](#), is used. You won't see these options without MDI deployed.

Let's check out the actions individually.

Confirm user compromised

If a user is marked as compromised, this integrates with Azure AD Identity Protection to mark the user as high-risk. What happens next is down to how you've configured Azure AD. For example, you may have a

Conditional Access policy that blocks high-risk users from signing in or otherwise limits their authentication rights.

Suspend user in AAD and Suspend user in AD

Suspending accounts in both Azure AD and on-premises AD keeps the account in the directory but blocks sign-in attempts. In Azure AD, it also blocks emails and calendar invites.

If users are synchronized from on-premises to Azure AD using Azure AD Connect, you may want to consider invoking both of these actions to work around the time it takes for the sync.

Force password reset

This option applies to on-premises users and applies at the next login, similar to the checkbox you can add to user properties in **Active Directory Users & Computers**. It's incompatible with accounts that have the **Password never expires** setting enabled, so you should check this when using it.

Require user to sign in again

When you choose this action, it is akin to the **Revoke sessions** option on Azure AD's user page. This revokes refresh tokens for Azure AD apps and services, meaning the user will need to re-perform authentication.

Now that we've covered device, file, and user responses, next, in the final section of this chapter, we will reiterate the features discussed in this chapter and how XDR differs from a traditional SIEM or niche SOAR solution.

How does M365D differ from a traditional SIEM or niche SOAR solution?

M365D differs from a traditional SIEM or a niche SOAR solution in several key ways.

First, M365D leverages a broad and integrated suite of Microsoft products, including MDE, MDO, and MDA, to provide end-to-end security coverage for organizations. This approach allows for a deeper and more comprehensive analysis of security events, as signals from different sources are correlated and analyzed together. In contrast, traditional SIEMs and niche SOAR solutions often rely on point products or limited integrations, which can result in blind spots and a lack of visibility.

Second, M365D's built-in automated response capabilities allow for immediate and real-time action to be taken against threats. The automated attack disruption feature, for example, leverages AI models to counteract the complexities of advanced attacks and contain them in real time, limiting their impact on an organization's assets. This capability is not typically found in traditional SIEMs or niche SOAR solutions, which may rely on manual intervention or limited automation.

Third, M365D's cloud-based architecture allows for more efficient and scalable security operations, as security events and data are analyzed and processed in the cloud rather than on-premises. This can result in faster detection and response times, as well as more effective threat hunting and investigation. In contrast, SIEMs and SOAR solutions generally may require significant on-premises infrastructure and resources, which can be costly and difficult to scale.

Overall, M365D provides a comprehensive and integrated security solution that leverages the power of AI and automation to enable faster and

more effective threat detection and response while also offering the scalability and efficiency benefits of the cloud-based architecture.

Summary

This chapter has been all about the XDR capabilities of M365D. We covered key aspects of XDR with Microsoft 365, focusing on using XDR to detect and respond to threats. Additionally, the chapter provides insights into best practices for optimizing XDR performance. By following the instructions in this chapter, organizations can enhance their security posture by effectively leveraging XDR capabilities within the Microsoft 365 environment. And I hope that you now know a lot more about how to operate the XDR parts in M365D than previously.

In the next chapter, we will take a deep dive into how to perform advanced hunting queries with KQL, and as a bonus, we will look at how to construct some custom detections as well.

Questions

To make sure you understand the extended detection and response subjects covered in this chapter, why not test yourself with the following questions?

1. Which of the following is a device response action? Choose all that apply:
 1. Isolate device
 2. Run an antivirus scan
 3. Delete the device
 4. Collect investigation package
2. Which of the following describes how an XDR differs from a SIEM solution?
 1. XDR platforms integrate with SaaS platform logs, but SIEM solutions cannot

2. XDR platforms do not have native response capabilities, but traditional SIEM solutions do
 3. An XDR can be offered as a managed service but a traditional SIEM solution cannot
 4. An XDR also adds the response capability, which a traditional SIEM solution doesn't provide natively
3. Which of the following is the last stage of incident response, and not one really covered by Microsoft 365 Defender?
1. Forensics
 2. Automated actions
 3. Recovery

Further reading

You may refer to the following links to expand your knowledge on the topics explored in this chapter:

- <https://learn.microsoft.com/en-us/microsoft-365/security/defender/incident-response-overview?view=o365-worldwide>
- <https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir?view=o365-worldwide>
- <https://learn.microsoft.com/en-us/microsoft-365/security/defender/automatic-attack-disruption?view=o365-worldwide>