Incident response playbooks

docs.microsoft.com/en-us/security/compass/incident-response-playbooks

- Article
- 04/28/2022
- 2 minutes to read
-

In this article

You need to respond quickly to detected security attacks to contain and remediate its damage. As new widespread cyberattacks happen, such as Nobellium and the Exchange Server vulnerability, Microsoft will respond with detailed incident response guidance.

You also need detailed guidance for common attack methods that malicious users employ every day. To address this need, use incident response playbooks for these types of attacks:

- Phishing
- Password spray
- App consent grant

- Compromised and malicious applications

Each playbook includes:

- **Prerequisites:** The specific requirements you need to complete before starting the investigation. For example, logging that should be turned on and roles and permissions that are required.
- **Workflow:** The logical flow that you should follow to perform the investigation.
- **Checklist:** A list of tasks for the steps in the flow chart. This checklist can be helpful in highly-regulated environments to verify what you have done.
- **Investigation steps:** Detailed step-by-step guidance for the specific investigation.

Also see Microsoft DART ransomware approach and best practices for information about how the Microsoft Detection and Response Team (DART) deals with ransomware attacks.

Incident response resources