Investigation, Alert, and Incident Selections

Learn why we close Investigations and Expel Alerts, and how we categorize Incidents.

Contents

Reason to Close (Investigations or Expel Alerts)

There are several reasons why we may close an Investigation or Expel Alert. **The specific options you see in the dropdown menu will vary depending on your location within Workbench.**

Reason	Meaning
PUP/PUA	■ Non-malicious files were identified as PUP/PUA at the time of the alert. ■ We only categorize as PUP/PUA if *two* or more of the following vendors identify it as such: Microsoft, Sophos, F-Secure, McAfee, Malwarebytes, Kaspersky, Symantec, McAfee-GW-Edition, BitDefender. ■ If two or more vendors do not indicate this categorization, it will be closed as a possible policy violation.
Possible policy violation	Could be any of the following: ■ Unauthorized activity that you are aware of and may have fixed/reverted (e.g. an engineer accidentally makes a resource publicly viewable, but the security team works with them to fix it). ■ A non-malicious file NOT identified as PUP/PUA. ■ Verified VPN activity, based source/destination IP or other parts of the alert (e.g. activity is on SurfShark VPN binary). ■ Piracy, pornography, or a productivity-impacting activity.
Testing	■ Verified internal testing activity.

Attack failed	■ An attacker made an attempt, but no compromise occurred. *You may be advised to take additional steps to mitigate any risk posed by the failed attack, or the attack could be considered "normal" enough (e.g. web scanning) that we do not recommend any additional steps.*
IT misconfiguration	■ Verified non-malicious activity was triggered by an IT issue, such as failed login attempts after an automated password change process.
Benign	■ A signature fired on a specific point-in-time activity that it was looking for (i.e. webshell request or psexec activity), but the context of the activity does not represent a threat. *Most behavioral signatures will fall into this category.*
False positive	■ The logic and intent of the signature did not align, and the signature needs to be reworked. *Examples include a login flagged as outside of the US, but the IP address is geolocated to Kentucky; or a binary flagged as malware, but the binary is a signature file.*
Other	■ Any reason that does not fit into the other categories. *In most cases, a specific close reason is added by an analyst.*
Inconclusive	■ You are unable to make a strong call one way or the other because you lack sufficient evidence.
Phishing Simulation	■ The alert or investigation was a confirmed phishing simulation. *This reason is unique to the Managed Phishing service.*
Suppressed	■ The alert has been automatically suppressed because it is a known benign issue.
Suppressed Manual	■ The alert has been manually suppressed because it is a known benign issue.
Suppressed New Device	■ The device is being tuned and is currently suppressed while the tuning process completes.

Suppressed Threshold Exceeded	■ The alert has been auto-closed because you have reached the threshold of alerts that can be associated with the investigation.
True Positive	■ The investigation or incident has been confirmed by you as true malicious activity or a valid threat.

Suspected Threat Type (Incidents)

The threat type indicates the type of activity that was observed for an Incident.

Type	Meaning
Targeted	■ The activity displays qualities of being targeted to your environment.
Non-targeted	■ The activity displays non-targeted qualities.
Policy violation	■ The activity indicates risky, user-driven behavior such as cryptocurrency mining or piracy.
Unknown	■ The activity is from an unknown threat at the time of promotion. *This status is subject to change during an investigation.*
Business email compromise (BEC)	■ The activity indicates a compromise of a business email account where the password was compromised, login was successful, *and* actions were successfully taken on a target. *This status is only used in situations where we can definitively confirm the threat vector was a phishing email and/or there was malicious activity observed within the email account.*
Non-targeted commodity malware	■ The activity displays non-targeted commodity malware qualities.
Red team	■ The activity is explicitly confirmed to be associated with red team engagement.

Credential theft	■ A password was stolen via credential harvesters, but the login was not successful and no actions were taken on the target (due to being blocked by MFA or conditional access).
Account compromise	■ A password was compromised, and login was successful. *This status is used when we cannot identify the threat vector/origin for a phishing email, or when the malicious activity is in your inbox or email account.*

Suspected Attack Vector (Incidents)

The attack vector indicates the vector of compromise identified for an Incident (meaning, what allowed the malware or actor into the environment).

Vector	Meaning
Drive-By download	■ The vector of compromise is a malicious download that occurred while visiting a malicious or compromised website.
Phishing	■ The vector of compromise is phishing activity.
Phishing - link	■ The vector of compromise is specifically a phishing link.
Phishing - attachment	■ The vector of compromise is specifically a phishing attachment.
Removable media	■ The vector of compromise is some type of removable media (like an infected USB drive).
Spear phishing	■ The vector of compromise is a targeted fraudulent email impersonating a trusted source.
Spear phishing - link	■ The vector of compromise is specifically a link in a fraudulent email impersonating a trusted source.
Spear phishing - attachment	■ The vector of compromise is specifically an attachment in a fraudulent email impersonating a trusted source.

Strategic web compromise	■ The vector of compromise is watering hole attack via an infected, trusted website.
Server-side vulnerability	■ The vector of compromise is a software infrastructure attack via a server.
Credential theft	■ The vector of compromise is theft of credentials.
Misconfiguration	■ The vector of compromise is an improperly secured resource that was left unintentionally exposed.
Unknown	■ The vector of compromise is unknown.

Suspected Attack Lifecycle (Incidents)

The attack lifecycle helps contextualize an Incident within the Cyber Kill Chain and MITRE ATT&CK frameworks. See About Detection Strategy in the Help Center for more information about these frameworks.

Stage	Meaning
Initial recon	■ The attack occurred during the Cyber Kill Chain's Reconnaissance stage.
Delivery	■ The attack occurred during the Cyber Kill Chain's Delivery stage.
Exploitation	■ The attack occurred during the Cyber Kill Chain's Exploitation stage.
Installation	■ The attack occurred during the Cyber Kill Chain's Installation stage.
Command & control (C2)	■ The attack occurred during the Cyber Kill Chain's Command & Control stage.

Lateral movement	■ The attack indicates Lateral Movement, per the MITRE ATT&CK framework.
Actions on targets	■ The attack occurred during the Cyber Kill Chain's Action on Objectives stage.
Unknown	■ The stage of the attack is unknown.