

Email Notification Template

Version: 1.0

Author: lucas salvatore

Notification Intent

- When where what happened, how bad is it
- what to do next
- All fields are **optional** but if it's **presented** then you must list it. List entries in descending order of **weight** or **priority** (use common sense, what info customers need to act on).

Initial Notification Template

MDR Case [Incident ID] Open: [Brief one line description about the case]

Tags: [Critical Threat|Critical Incident|NonCritical Threat|NonCritical Incident] [PowerShell Execution] [Obfuscation] [Other] (indicate **Severity Level** through here)

Summary

[Provide a concise description of the detection, including the suspected threat, execution context, affected endpoint, and relevant indicators.]

Impact

Impact type	Use when	Standard wording
No impact identified	Activity was detected, but no effect is known	No security or business impact has been identified.
Potential impact	Harm is possible but not confirmed	[Asset/account/data] may be affected.
Confirmed impact	The effect has been verified	[Asset/account/data] was affected by [activity].
Operational impact	A service, system, or business process is disrupted	[Service/system/process] is experiencing [degradation/outage/disruption].
Access impact	Unauthorized access may have occurred	Unauthorized access to [system/account] may have occurred.
Credential impact	Credentials may be exposed or misused	Credentials for [user/account] may be compromised.
Data impact	Data may have been accessed, changed, deleted, or transferred	[Data type] may have been [accessed/modified/transferred/deleted].

Impact type	Use when	Standard wording
Endpoint impact	A device may be compromised or affected	[Endpoint] may be compromised or unavailable.
Network impact	Malicious or unusual network activity is involved	[Network segment/system] may be exposed to unauthorized communication.
Scope impact	Multiple assets, users, or systems may be involved	Activity may extend to [number/type of assets].
Contained impact	The threat was stopped or isolated	The affected [asset/account/connection] has been contained.
Ongoing impact	The threat or business effect is still active	The impact is ongoing and continues to affect [scope].
Unknown impact	The effect has not yet been determined	The potential impact and scope remain under investigation.
Resolved impact	The incident is closed and no continuing effect exists	The incident has been resolved; no continuing impact has been observed.

Analyst selection rule

Select:

1. One primary impact type
2. One scope
3. One certainty level

Complete the following sentence:

> **Impact:** [Impact type] affecting [scope]. [Business or security consequence]. [Current status or certainty].

Examples

- **Impact:** Potential credential impact affecting one user account. Unauthorized access cannot be ruled out.
- **Impact:** Confirmed endpoint impact affecting one workstation. The device has been isolated from the network.
- **Impact:** No impact identified. Malicious network traffic was blocked before successful access was confirmed.

Action Plan

for now must be case specific, hand written, as MDR generated narratives are not usable, can use help of AI but don't paste any PII

Examples

- Contain or quarantine the malicious PowerShell script.
- Isolate the affected endpoint from the network if active execution or lateral movement is suspected.
- Terminate related PowerShell processes and review parent-child process relationships.

Context info

Endpoint IP (if applicable): 10.0.60.117

Endpoint Hostname (if applicable): Contoso

Endpoint ID (if applicable): 1234567

File Path (if applicable): C:\Windows\system32\powershell.exe

Commandline (if applicable): powershell -e JABjAGwAaQBlAG4…

File MD5 (if applicable):

Src IP (if applicable):

Dest IP (if applicable):

Packet Proof (if applicable):

First Detected: Do 3. Sep 12:08:53 CEST 2026

Detection Source: [Type: Endpoint Secure | STA | etc.] | [ID]

Owner and Escalation path: [Assigned T1 T2 T3 analysts name and email addresses]