Cybersecurity and Privacy Incident Report Template

[This template aims to help incident responders capture key details about a cybersecurity or data privacy incident. You should customize it to meet your needs. The text in square brackets is meant to guide you; remove it before finalizing the report. The title above is generic; change it to be specific to the incident, possibly by summarizing the nature of the incident.]

Alert / Detection Details

Case / Ticket ID	
What was the detection source? (XSIAM, MDE, etc.)	
What was the initial alert name / rule	
Were there related alerts or correlated activity across tools? (e.g., XSIAM, MDE)	
Who is the response coordinator for this incident?	[The incident response coordinator is typically the person in charge of the response effort and the primary author of this report.]
What was the nature of the incident?	
When did the incident occur?	[Specify the date, start, and end time, and time zone.]
Which specific IT resources were at risk?	[Examples include an application, employee laptop, server, network device, etc.]
What business processes were affected?	

What is the severity or significance of the incident?	
Which third parties, such as vendors or customers (if any), were involved in or affected by the incident?	
Did the incident result in the destruction or unauthorized disclosure or access of what might be considered personal data or personally identifiable information (PII)?	[If yes, describe the type of data that was affected (e.g., employee information, customer contact details, customer electronic data, etc.) and how it was affected (e.g., unexpected destruction, access, etc.).]
What might be the cybersecurity or privacy risks to the parties affected by the incident?	[Examples of the risks include identity theft, increased chances of a follow-up attack, damage to reputation, disclosure of sensitive data, etc.]
In which geographic regions was the affected data located?	
Who are the business owners and key stakeholders of the affected resources or data?	

What Was the Root Cause?

What is your initial working theory (hypothesis) about the cause (even if not confirmed yet)?	
What caused the incident?	
How do we know?	

How confident are we in the assessment?	
What connections exist to past incidents, if any?	

What Was and Remains to Be Done?

Containment: How were we able to limit the incident's scope, including adverse effects on the affected data and systems?	
Eradication: What steps were taken to eliminate adversarial presence from the affected environment, protect the affected data, or minimize the risks to the affected parties?	[Such steps might include deleting malware, restoring trusted backup, deleting a sensitive file from an unauthorized location, etc.]
Recovery: How and to what extent did we restore normal business operations or normal data processing activities?	

What Lessons Can Be Learned?

How could the involvement of people help mitigate our future risks?	
How might we adjust processes to prevent the problem or allow us to respond better?	

How might we use technology to enable us to improve?	
How might new IOCs (hashes, domains, cmdlets) be shared with detection engineering or threat hunting teams?	

What Are the Remaining Action Items?

Action	Responsible Party	Expected Start Date

Report Changelog

Date	Author	Change Description

About this Document