Design by Paradigm | Incident Reporting Template

SECTION A: INCIDENT DETAILS				
Incident number(s):	HDE-1001, HDE-1050, HDE-1072			
Incident date(s):	13 DEC 10:00 a.m. | 13 DEC 3:14 p.m. | 13 DEC 3:20 p.m			
Report author:	011480496			
Report date:	1/21/2024			
Summary of incident:	Received helpdesk tickets regarding slow performance of the engineering application used to render files. The operations team rebooted the server storing engineering files, but continued to face latency issues. After verifying that engineers were using the latest software version, the issue was escalated to my team. I discoved that recent updates were installed on the struggling server, and the administrator downloaded them from an email that appeared to be from the vendor's expected contact. However it was later found that email was sent from a personal address spoofing the vendor's contact. After logggin into SIEM tool, I observed high GPU and CPU usage on the server both during and after office hours. Additionally, unauthorized remote network connections were established between server and an unknown IP address.			
Impacted system(s):	WIN-6JNN6RLT6IL, server-2016-3, Server_Firewall.localdomain			
Primary function of the impacted system(s):	CAD application – the use of computer-based software to aid in design processes. Engineering.			
Impacted user(s):	Maya Patel, Diego Martin, Alex Lee			
Incident timeline:	13 DEC 10:00 a.m. | 13 DEC 3:14 p.m. | 13 DEC 3:20 p.m			
Functional impact: (*See section: Glossary*)	☒HIGH	☐MEDIUM	☐LOW	☐NONE
Incident priority:	☒HIGH	☐MEDIUM	☐LOW	

Additional notes:	13

Incident type: (*check all that apply*)

☒Compromised system	☐Lost equipment/theft
☐Compromised user credentials *(e.g., lost password)*	☐Physical break-in
	☒Social engineering *(e.g., phishing)*
☐Network attack *(e.g., DoS)*	☐Law enforcement request
☒Malware *(e.g., virus, worm, Trojan)*	☐Policy violation *(e.g., acceptable use)*
☐Reconnaissance *(e.g., scanning, sniffing)*	☐Other: Click or tap here to enter text.

SECTION B: DETECT	
Hostname of the impacted system(s):	WIN-6JNN6RLT6IL
IP address of the impacted system(s):	10.10.20.10
Operating system of the impacted system(s):	Microsoft Wiindows Server 2019 Standard 10.0.17763

SECTION C: INVESTIGATE	
Destination port of malicious traffic:	3333
Additional notes & observations:	It shows additional data such as timestamp, date, time, log, agent id, rules etc.. I believe the CAD application is compromised with malware.

SECTION D: REMEDIATE	
Summary of actions taken to restore functionality of impacted system(s):	Remediated the incident by terminating any high-resource processes, restoring antivirus functionality, and updating firewall policies
Summary of actions taken to restore network security:	Restored Windows Defender Antivirus. Updated Server Firewall to add more rules for the security system. Did threat hunting to find and eradicate the existing malware causing work stoppage.`

Additional notes & observations:	N/A

SECTION E: LESSONS LEARNED			
Recommendation for preventative actions:	**ACTION**	**NEGATIVE IMPACT ADDRESSED**	**PREVENTION METHOD**
	1. Antivirus program	Latest version of software/ Latency issues.	Preventative Controls
	2. Employee Security Awareness Training	Recognize Spoofing attempts and verifying actual programs/updates	Preventative Controls
	3. Server Firewall	Deny any harmful programs. Deny all	Deterrent Controls
	4.		

Glossary

Functional Impact

Functional impact categories to prioritize resources in incident response:

CATEGORY	DEFINITION
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide critical service to a subset of system
High	Organization is no longer able to provide some critical services to any users