Design by Paradigm | Incident Reporting Template

SECTION A: INCIDENT DETAILS	
Incident number(s):	HDE-1001, HDE-1050, HDE 1072
Incident date(s):	13 DEC
Report author:	011553812 Tyra Austin
Report date:	8/16/2024
Summary of incident:	Pro-Engineer Application is not working for any employees. It is not allowing the employees to access model files in the server, and the application is running slow and timing out. Causing a work stoppage.
Impacted system(s):	WIN – 6JNN6RLT6IL
Primary function of the impacted system(s):	Updates the model files
Impacted user(s):	Maya Patel, Diego Martin, Alex Lee
Incident timeline:	13 DEC :10am, 3:14pm, and 3:20pm
Functional impact: (*See section: Glossary*)	☒HIGH ☐MEDIUM ☐LOW ☐NONE
Incident priority:	☒HIGH ☐MEDIUM ☐LOW
Additional notes:	n/a

Incident type: (*check all that apply*)

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

SECTION B: DETECT

Hostname of the impacted system(s):	Server-2016-3
IP address of the impacted system(s):	10.10.20.10
Operating system of the impacted system(s):	Microsoft Windows Server 2019 Standard 10.0.17763

SECTION C: INVESTIGATE

Destination port of malicious traffic:	3333
Additional notes & observations:	Data destination IP: 159.203.162.18

SECTION D: REMEDIATE

Summary of actions taken to restore functionality of impacted system(s):	Used the Task manager to see what was using all the CPU memory found a process called (XMRig miner). Looked at the search onile and the file location.
Summary of actions taken to restore network security:	Turned off the Windows Defender Antivirus and reinstalled the virus & threat protection Which removed the file form the computer.
Additional notes & observations:	Then I added a new firewall rule to the DMZ to block TCP/UDP traffic from leaving the network.

SECTION E: LESSONS LEARNED

Recommendation for preventative actions:	**ACTION**	**NEGATIVE IMPACT ADDRESSED**	**PREVENTION METHOD**
	1. Unauthorized devices having access to the server	Disrupt normal business hours	Regular Security Audits
	2. Isolating the critical assets	Impact on Network performance	Network Segmentation

	3. Phishing attempts to gain access to systems	Compromise of Networks systems	Annual employee training, email filtering
	4. Correctly detect and identify unauthorized access attempts	Potential for Blind spots, and alert fatigue from false positives	HIDS/IPS

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