D483 Task 1 Background Information

Security Operations Scenario

You are a security professional working in incident detection and response at the manufacturing company Design by Paradigm. An engineer at the company submitted a helpdesk ticket after the application used to render engineering files began performing slowly. The operations team recognized that the server storing the engineering files was experiencing high utilization and rebooted the server as part of the standard operating procedure. Following the server reboot, additional helpdesk tickets were submitted by engineers still experiencing latency issues. After the support technician verified that each engineer was running the latest version of the software, the helpdesk tickets were escalated to your team and assigned to you.

You began your investigation by reaching out to the applications engineering group, discovering that updates were recently installed on the struggling engineering application server. The administrator who installed the updates commonly receives vendor updates by email and admitted they did not verify the sender before downloading the updates. The email containing the system update links appeared to come from the expected vendor contact who regularly sends out update notices. Upon closer examination, it was discovered that the update email was sent from a personal email address spoofing the expected contact's vendor email address.

After the call, you log into your security information and event management (SIEM) tool and notice unusually high GPU and CPU usage on the engineering application server, both during and after office hours. You observe that remote network connections have been established between the server and an unknown IP address.

Continue the investigation by logging into the virtual lab environment to view the SIEM tool dashboard. You will use the tools given to investigate the suspicious activity on the server. The provided "Incident Reporting Template" will document your findings regarding the scope of the incident and corrective actions that could resolve the issue and prevent similar events from occurring in the future.

The intended audience of your incident report is the stakeholders at Design by Paradigm.

Helpdesk Ticket Artifacts (3)

Support Ticket HDE-1001

Incident Number:	HDE-1001
Incident Date/Time:	13 DEC 10:00 a.m.
Name:	Maya Patel
Email:	m.patel@designbyparadigm.com
Services Disrupted:	CAD Application
System Name:	WIN-6JNN6RLT6IL
Priority:	High
Duration of Interruption:	Ongoing
Major Incident:	No
Additional Details:	Employee states she is unable to use the Pro-Engineer application to update models. She says the application is running slow and timing out, creating a work stoppage.

Support Ticket HDE-1050

Incident Number:	HDE-1050
Incident Date/Time:	13 DEC 3:14 p.m.
Name:	Diego Martin
Email:	d.martin@designbyparadigm.com
Services Disrupted:	CAD Application
System Name:	WIN-6JNN6RLT6IL
Priority:	High
Duration of Interruption:	Ongoing
Major Incident:	No

Additional Details:	Employee states he is unable to use Pro-Engineer to update models. He has tried multiple model files, so it is not his machine or one specific model file. He is at a work stoppage.

Support Ticket HDE-1072

Incident Number:	HDE-1072
Incident Date/Time:	13 DEC 3:20 p.m.
Name:	Alex Lee
Email:	a.lee@designbyparadigm.com
Services Disrupted:	CAD Application
System Name:	WIN-6JNN6RLT6IL
Priority:	High
Duration of Interruption:	Ongoing
Major Incident:	No
Additional Details:	Employee is unable to use Pro-Engineer to update models. Employee used Task Manager to end the program, but after restart of Pro-Engineer, the same issues are still happening with multiple model files. The application is running slow and timing out, and the employee is concerned there is a problem with the server. Employee is at a work stoppage.