What is SIEM?

SIEM Security Information and Event Management it is a comprehensive system which generates, analysis and manage the security data from any different resources across the entire IT infrastructure. It is the combination of both Security Information Management and Security Event Management, so together they form a unique platform which offer real-time monitoring, historical analysis and automated incident response.

What is SIEM Alerts?

When SIEM identifies a threat, it sends an alert with a defined level rules to help analysts to prioritize the next steps.

Alert : Malware Detected on Endpoint

Step 1: Initial Triage
Step 2: Data Collection
Step 3: Initial Analysis
Step 4: Deep Dive Analysis
Step 5: Containment and Mitigation
Step 6: Eradication
Step 7: Recovery

Explanation: Examine the alert to understand which endpoint is affected, the type of malware detected. Collect relevant logs from the affected endpoint to analyse the malware detection. Determine if the user performed any actions that lead to malware infection. Use various OSINT tools to gather more information about the detected malware, if the malware is confirmed malicious, isolate the endpoint to prevent further spread, run a full scan anti-malware to remove the threat from the endpoint, Confirm the root cause is eliminated completely, and finally restore the data from backups and connect the cleaned secured endpoint to the network and monitor for any further issues.