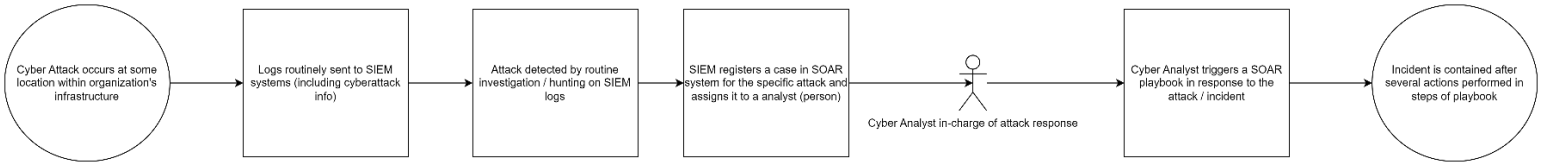
Title: Using Generative-AI for Cybersecurity Incident Response Recommendations

AI for Business: Team 5

Current version of automated Cyber-threat detection and response process:

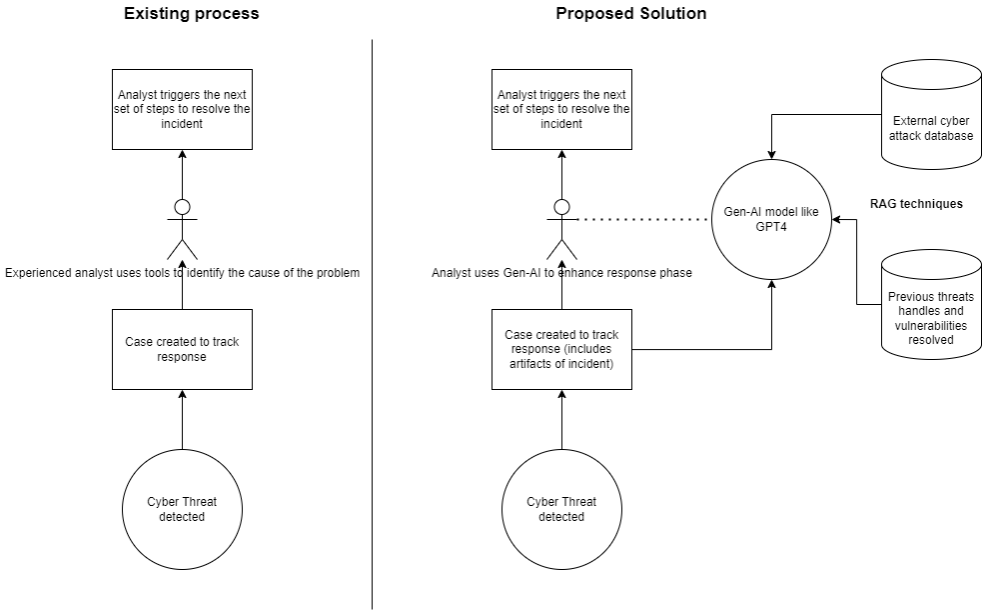


Link to diagram: https://usf.box.com/s/ldzefz27qad6riaaa5tjifiewhkfdhbe

Logs are actively collected from various devices in a company's infrastructure and sent to an analysis system like SIEM (Security Information and Event Management). These logs are routinely scanned and analyzed for anomalies to hunt down threats. Once a threat / attack is detected, the SIEM system creates a case / ticket in an incident response system like SOAR (Security Orchestration, Automation and Response) and adds all artifacts associated with that threat to case. When a case is created, either a series of response steps are triggered automatically (automation) or an analyst utilizes a dynamic playbook to resolve the incident (orchestration).

Potential for AI:

The reason why the cybersecurity response is not fully automated, is because they are complex processes and there is no one-fits-all solution for every organization. Cybersecurity analysts are intermediate agents who make sure that the correct set of steps are triggered, and the incident is properly contained. Sometimes there are incidents occurring that have never been reported and documented before. These incidents are called '**black swans'** and take longer to resolve primarily because they are unconventional and the appropriate response for the attack is not documented. For this type of incident, cybersecurity analysts usually must scour through documentation, consult external security agencies to locate the vulnerability. This is a long process and increases the time it takes to recover, costing the company a lot of money every passing second. Generative AI helps greatly in this process by acting as a **recommendation engine** from which analysts can benefit from.



Link to diagram: https://usf.box.com/s/4rynoibsnvbt3n049onp9a914xqpybln

Plan for diagnosis phase: Identify and document how cybersecurity analysts work to resolve black swan incidents.

Plan for design phase: Explore Gen-AI tuning steps to make it provide accurate diagnosis for cybersecurity threats.

References:

https://telefonicatech.com/en/blog/cybersecurity-black-swan-events-in-a-connected-world

https://lantern.splunk.com/Security/Product_Tips/SOAR/Managing_cases_in_SOAR

https://www.financierworldwide.com/preparing-for-a-black-swan-cyber-event

https://www.youtube.com/playlist?list=PLOspHqNVtKADkWLFt9OcziQF7EatuANSY