Security Analyst Intern

SGP Project - Semester 7

-By Poojan Shah (19IT133)
-Mentor- Prof. Madhav Ajwalia

Table of contents

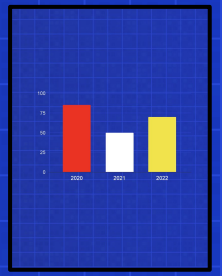
About Internship project

Working as an Associate Security Analyst – Intern at SharkStriker INC includes the following roles and responsibilities

- Continuous alert monitoring and identifying vulnerable or suspicious activities of an adversary. If incident happens, immediately respond to that incident on the ticketing portal.
- Also, proactive and leadless threat hunting as a part of threat intelligence to detect any residual risks in a system or network and if found, take necessary preventive steps for rule creations in SIEM and responding to its incident.
- Train for Vulnerability Assessment and Penetration Testing (VAPT) for upcoming projects and refer to good write ups.
- Also, managing EDR (Endpoint Detection and Response) and SIEM (Security Information and Event Managemement) to True Positive, False Positive, True negative, False negative alerts.

Monitoring Alerts

Why it is important and how alerts are monitored ?



- Monitoring alerts across the network for all the end devices including workstations, servers, firewalls, IDS/IPS traffic, Web traffic and many other categories that are suspicious or have triggered to such suspicious conditional behaviour.
- To find root cause of alerts based on various different parameters and find whether it is False positive or alert is actually a True positive.
- If False positive, fine tune the SIEM rules to reduce FP and also improve the alert monitoring by reducing fatigue in it.
- Also, to create dashboards in SIEM for various different purposes for analyzing traffic across different network categories

SIEM

- Security Information and Event Management (SIEM) tool is one of the main part for triggering and handling the logs and alerts across network.
- There are various predefined rules created by the SIEM itself for many different known attacks but responsibility of the Security Analyst is to create custom rules in SIEM so that alerts are triggered when an anomaly takes place.
- Also, the MITRE framework is used to map these Tactics, Techniques and Procedures (TTP's) to get analyst better analysis about the attack or any anomaly and also in most of cases is necessary and good practice.
- Also, SIEM has capability of creating visualization dashboards so that analysts can get ease at work to identify and known or unknown anomalous behaviour

VAPT

- VAPT training includes to solve the labs that gives practice to find vulnerabilities in the Web Application.
- OWASP Top 10 are considered as the prior and standard vulnerabilities for be found in any VAPT assessment conducted.
- Also, the penetration testing involves a proper predefined template of report which gives idea in very detail about impact of the vulnerability along with POC (Proof of Concept).
- To get upto date with bug bounties write ups to see how different professionals find different vulnerabilities in application and get some learning curve from it.

EDR

- EDR (Endpoint Detection and Response) are those capable tools that are responsible to specially monitor Endpoints like windows workstations and triaging alerts for it.
- Also, some part of Endpoint detection includes an investigation where in if any malicious activity has taken place, analyst of responsible to carry out complete investigation on it from EDR and also give necessary output.
- Also, EQL (Event Query Language) is used by some EDR's that is used to query across systems across the tool and find necesary results.
- Also, if EDR supports EQL, custom rules are created in it to tigger any activity if or not performed by an adversary.

Threat Hunting

- As a part of proactive threat intelligence, threat hunting is one of those job that keeps the analyst aware of what activity is going on in the network.
- Also, threat hunting are of different kinds: 1) Leadless Hunting 2) Lead based hunting
- If any anomaly is found during these hunts, then that incident is reported immediately and also necessary prevention rules and techniques are created and conducted to prevent those anomaly from spread furthermore.
- Threat hunting also gives a detail insight of the activity going on in the network and gives capability to study behaviour patterns.

ThankYou