COMP3010 COURSEWORK 2

BOTSv3 incident analysis and presentation

(s) Samuel Honeybone
[Email address]

Contents

Introduction

Security operations centres (SOCs) are vital in the modern world of cyber security. They are a cyber security team which monitors an organisations IT infrastructure 24/7 with the aim of finding, analysing and responding to potential security incidents as they happen. (Mark Scapicchio et al, N.d.) This helps to improve companies' response time to cyber events and help to prevent future attacks as the monitoring can find the weak points in the infrastructure that cyber criminals are trying to exploit.

This report will cover the investigation of an event which happened in the BOTSv3 dataset, a publicly available and pre-indexed security dataset with many different security events such as DDoS attacks. This report will specifically focus on a cloud misconfiguration event which could have led to data exposure where a S3 bucket was made public for anyone to interact with.

The analysis of this event will be done with Splunk as the primary security and event management (SIEM) solution and will focus exclusively on cloud related events and works on the assumption that the business is a medium sized company with less than 100 employees working for them.

SOC roles and incident handling reflection

Within a SOC the analysts are generally split by tiers, these tiers range from tier 1 through to tier 3. The lowest of the 3 tiers is tier 1 which is generally considered the easiest role to perform and requires the least amount of experience to get a role within. The general responsibilities of a tier 1 SOC analyst is to monitor the alerts and traffic on the network to look for any issues or flags which may occur, when they see these errors such as an antivirus flag or an Intrusion detection/ prevention systems rule being breached when they find these events they need to sort them by priority and if necessary escalate them to the tier 2 analysts. (Paloalto Networkd, N.d.)

The tier 2 analysts are the next step up from the tier 1 analysts their role is to review higher priority security incidents which have been escalated to them via the tier 1 analysts and perform a more in-depth analysis on them discovering the affected systems and coming up with a plan to contain and bounce back from the incident. (Connect Wise, N.d.)

Finally tier 3 analysts actively hunt for threats trying to discover areas where a network may be weak through things like penetration testing and they aim to suggest improvements to the networks current security to prevent future attacks. In the event a tier 2 analyst can't handle an issue they will be dealt with by a tier 3 analyst. This tier also must investigate the alerts and other data provided to them by tier 1 and 2. (Paloalto Networkd, N.d.)

In context of the BOTSv3 scenario, the tier 1 analysts would generally monitor the infrastructure looking for suspicious activity such as API calls being made without multi factor authentication or suspicious changes to the S3 buckets access controls, when they noticed something like this happening they would then escalate it to the tier 2 analyst who would look deeper into the incident trying to discover the involved user and as well as the effected systems, such as which S3 bucket was effected and whether anything was uploaded to the bucket in the time that it was public. Finally, the tier 3 analyst would investigate the potential ramifications for the business and recommend setups which could be implemented in the future to prevent incidents like this happening again such as setting up more strict user settings and mandatory multi factor authentication (Amazon web services, N.D.).

Installation and data preparation

Guided Questions

Conclusion

References

There are no sources in the current document.