LOGPOINT

LOGPOINT CTF

DATE: AUG 28, 2023

PRESENTER’S NAME: PRABESH BHATTA

PRESENTER’S TITLE: ASSOCIATE ENGINEERING MANAGER (CUSTOMER SUCCESS)

What is Logpoint CTF (Capture The Flag) ?

- CTF is a kind of information security competition that challenges contestants to solve a variety of tasks.
- We will be looking into cyber security events via the perspective of security analyst utilizing SIEM.
- All the flags can be obtained on SIEM (Logpoint) itself.
- CTF will be conducted on team.

Possible CTF Challenges

- Detection of possible brute force Attacks.
- Ransomware Attacks.
- Detection of insider threat.
- Detection of Possible Phishing Attacks.
- Suspicious behavior of log source.
- Exfiltration

CTF Details

Think Like a SOC Analyst

Challenge Category

- TOTAL QUESTIONS (~40 Questions)

These might include bonus questions which comes after you correctly answered certain questions.

Scoring Criteria

Each question (+5)

Some hints cost points (upto -4)

Total Duration:– 3 hours

CTF Demo

1.Many of our employees got “yearly BONUS” themed emails. The emails were not filtered as spam and we suspect many of our employees got the email. What was the subject of those emails? Log source: Office365 email

Chart count() by norm_id

bonus

2. Ransomware attack detection by Trend Micro Deep Security.

Trend Micro Deep Security has detected a ransomware attack on our organization. What is the name of the impacted workstation.

Log Source: Trend Micro Deep Security

Chart count() by norm_id

Hint: look for host

3. Find the username, device_ip of a user which have most number of successful user login in windows system.

Log source: Windows/Sysmon

Chart count() by label

CTF Demo

1. What is the IP address of the machine with most RDP connections on last 6 hours? Hint: search through event ID
2. An attacker disabled defender firewall running in a workstation. What was that workstation's name ?

Hint: event_id=5001

Resources

Session on Logpoint queries and pattern finding:

Study Materials:-

https://docs.logpoint.com/docs/search-query-language/en/latest/index.html

Do you have any queries?

Thanks!!