SIEM 101 BY P3NGU1N

Log Collection

🎯 What is the best method for those who do not want to manage agent software?

ANSWER: agentless

🎯 “Universal Forwarder” is the agent software of which product?

ANSWER: splunk

Log Aggregation and Parsing

🎯 Which one is not the skill of a log aggregator?

- filtering
- parsing
- analysis
- enrichment

ANSWER: analysis

🎯 What is the EPS of a SIEM system that receives 150000 logs per minute?

ANSWER: 2500

Log Storage

🎯 Is data update (change value, delete value etc) very important for SIEM data storage?

ANSWER: N

🎯 Which one is the most important for SIEM storage?

- Speed
- Features
- Price

ANSWER: speed

Alerting

🎯 I have 2 IP addresses that are certain to be malicious. I want to create an alert when these are accessed. Which method should I use?

- whitelisting
- blacklist
- long tail

ANSWER: blacklist

🎯 "The whitelist method is not only very effective but also very easy to manage." Is that true or false?

ANSWER: false

QUIZ:

🎯 **Which is not the log collection method?**

ANSWER: **Via USB Drive**

🎯 **Which one is not the cons of agentless log collection?**

ANSWER: **No required log collection software**

🎯 **Maximum packet size that can be sent with Syslog UDP is ..... bytes**

ANSWER: **1024**

🎯 **Which one is not the skill of log aggregator?**

ANSWER: **Analysis**

🎯 **You are using hash blacklist for 'mimikatz.exe'. How to attacker can bypass it?**

ANSWER: **echo 1 >> mimikatz.exe**

🎯 **Select correct one about whitelist method**

ANSWER: **Highly effective but difficult to manage**

🎯 **Why indexing is important for storage technology?**

ANSWER: **Fast access to data**

🎯 **Which one is correct about long tail analysis?**

ANSWER: **Least common events are most useful**

🎯 **Select correlation about brute force attack**

ANSWER: **15 Login failed in 1 minute with the same IP address**

🎯 **Which is one of the features you should pay attention to when storing log?**

ANSWER: **Search speed**