Blue Team Level 1 Certification (Standard)
12 Topics | 1 Quiz
PA7) Report Writing
7 Topics | 1 Quiz
PA8) Phishing Response Challenge
3 Topics | 1 Quiz
THREAT INTELLIGENCE DOMAIN
TI1) Introduction to Threat Intelligence
7 Topics
TI2) Threat Actors & APTs
6 Topics | 2 Quizzes
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
Section Introduction, Correlation
Normalization and Processing
SIEM Rules
Sigma Rules
Regex
Activity) Writing Sigma Rules
Activity) End of Section Review, Correlation

SIEM Rules

What are SIEM Rules?

SIEM rules typically come in two forms; rules that are provided by the SIEM provider to offer 'out-the-box' functionality to detect generic attacks and suspicious patterns, and human-written rules that are developed by the defenders from the organization as they understand what is normal activity, and what isn't. But what actually are they? They are search queries that are looking for specific activity, looking at any imported or real-time data that is being fed into the SIEM solution. If the rule query matches a piece of data, different actions can be triggered, such as generating an alert, sending an email to a team, or recording the activity to a separate location. These search queries can be running continuously (real-time detection), or set to run at specific scheduled times, such as every day, or every week.

Examples of SIEM Rule Functionality

We can create rules to detect an endless amount of activity, providing the SIEM is pulling in the required logs. Below are just some of the things we can monitor for:

Authentication/Account Activity:

- Failed logon attempts
- Successful (or failed) login attempts to disabled accounts
- Use of specific accounts (local administrator, administrator, domain administrator)
- SID (Security Identifier) changes to an account (a potential indicator of privilege escalation)

Process Execution:

- Execution from unusual locations (such as temporary directories or browser caches – may indicate malware execution or persistence mechanisms)
- Suspicious process relationships (such as Microsoft Word spawning a child process of CMD or PowerShell window (potentially a malicious macro that is executing code))
- Known bad hashes (MD5, SHA1, SHA256 hashes that are generated from confirmed malicious files)

Network Activity:

- Port scans
- Service enumeration
- Host discovery

False Positive Reduction and Tuning

False positives are alerts that have generated but do not actually represent a malicious event. An example of this would be a rule that is monitoring Windows Event ID 4625 – 'An account failed to log on'. Monitoring this log will tell us when an account fails to login successfully. Everyone has entered their password in wrong once or twice, so creating a rule that looks for single occurrences of login failures isn't going to provide much value, and will be very noisy (meaning it will generate a LOT of alerts). Thresholds can be set to allow for more control over what happens when searches bring back results from the aggregated data. We can set a rule threshold, so if an account fails to log in 10 times within 10 minutes, then generate an alert. This can help us to identify attacks where a malicious actor is trying to log into an account by guessing the password (brute-force or dictionary attacks).

In some cases the rule may need to be altered to specify that some values should be ignored. Let's go through an example; we have a rule that looks at firewall logs to identify network scanning activity where one source IP is sending traffic to a high number of internal systems. Our company then purchases a vulnerability scanner and sets it up in an internal network, planning to perform host discovery scans to actively identify running systems so this

SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam

information can be stored and used to plan vulnerability scans in the future. While the scanner is sending traffic to every potential IP in it's defined target range this rule is going to alert on activity that isn't malicious – if the security team deems it appropriate they can choose to exclude this source IP from the rule. So now when the scanner activates the activity will be observed by the SIEM but the rule is telling it not to alert when this specific source IP is seen – we have now prevented future false positives from generating.

Writing Search Queries and Alerts

We're going to cover this in the next section, where you'll set up your own local version of Splunk SIEM, and learn how to write search queries to find specific information within a dataset that contains hundreds of thousands of logs. Once you know how to write search queries, you can apply this to set up alerts!

Before you jump into that section we recommend reading this page on creating detection rules in the ELK stack, an open-source SIEM alternative. While we're going to be using Splunk, this will definitely give you a great insight into the logic behind rules! – Creating detection rules | Elastic Security Solution [7.9] | Elastic

Previous Topic
Mark Complete
Next Topic
Back to Lesson