

Blue Team Level 1 Certification
(Standard)

7 Topics

✓ Security Controls

5 Topics 1 Quiz

✓ Networking 101

6 Topics 1 Quiz

✓ Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

✓ PA2) Types of Phishing Emails

10 Topics 2 Quizzes

✓ PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

✓ PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

✓ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

○ PA6) Taking Defensive Actions

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) ...

Sigma Rules

Blue Team Level 1 Certification (Standard) > SI4) Correlation > Sigma Rules

IN PROGRESS



Sharing SIEM rules can be an extremely beneficial process for a security team, whether they're sharing them or retrieving them, but SIEM rules are written in specific structures depending on the SIEM platform. While it's possible to share the logic of the rule (how it works) in plain English, there is a better way to quickly share or ingest SIEM rules shared by teams around the world. In this lesson we're going to introduce you to Sigma.

To ensure accuracy we've copied information directly from the Sigma Github page available [here](https://github.com/Neo23x0/sigma).

What is Sigma?

Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.



<https://github.com/Neo23x0/sigma>

Rules can be written in the Sigma language and then using a converter (Sigmac) they can be exported as rules in the correct format for a number of different SIEM platforms. This process can also be reversed allowing security professionals to export rules from their vendor format to Sigma format so they can be used by teams with a different SIEM.

Which Platforms Support Sigma?

- Splunk
- QRadar
- ArcSight
- Elasticsearch (Elasticsearch, Query strings, DSL, Watcher, & Kibana)
- Logpoint

Benefits of Using Sigma

- Describe your detection method in Sigma to make it sharable
- Write your SIEM searches in Sigma to avoid a vendor lock-in (meaning you can flexibly change SIEM solution without having to lose all of your custom rules)
- Share the signature in the appendix of your analysis or research report along with IOCs and YARA rules to

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

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

- Share the signature in the appendix of your analysis or research report along with IOCs and TIVs rules to allow others to replicate your work and build detection rules
- Share the signature in threat intel communities (ISACs) – e.g. via MISP (which we covered in the Threat Intel domain!)

SIGMA Rule Example

In this example we're looking at a Sigma rule that can detect when a web server has been compromised and is running a web shell, allowing a malicious actor to visit a specific URL which will provide them with a console, allowing them to execute commands as if they are on the server. We'll break down the rule below, even though it's really human-readable!

```
1 title: Webshell Detection by Keyword
2 description: Detects webshells that use GET requests by keyword searches in URL strings
3 author: Florian Roth
4 logsource:
5   type: webserver
6 detection:
7   keywords:
8     - 'whoami'
9     - 'netcat20user'
10    - 'cmd20/c20'
11   condition: selection and keywords
12 falsepositives:
13   - Web sites like wikis with articles on os commands and pages that include the os commands in the
14     URLs
15   - User searches in search boxes of the respective website
16 level: high
```

On line 6 we can see that the 'detection' is declared, stating how this rule works. Line 7 states it is using the method of matching keywords against a URL string (mentioned on Line 2).

So if this rule was actively being used to monitor a web server and we had a web shell running on <https://example.com/13919595/asjkdasjdkasjvn/shell.php?>, and we visited the interface and tried to use the command 'whoami' this would be included in a POST HTTP request to the web server, meaning the URL will be changed to include 'whoami'. This activity would generate an alert for the security team to investigate, making them aware of the web shell. It is extremely unlikely that a normal visitor would ever need to include these operating system commands in a POST URL request so there is a low rate of false positives (but some scenarios are covered on lines 13 and 14).

There are some great real-world rules to take a look at on Florian Roth's Github page [GitHub – Neo23x0/sigma: Generic Signature Format for SIEM Systems](#). Additional rules are available at <https://github.com/SigmaHQ/sigma/tree/master/rules>. We highly recommend taking a look at these to better understand how they function.

< Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic >