Master of the SOC

Cybersecurity

SIEM Day 6

Today, we will review many SIEM and Splunk concepts and tools in a comprehensive activity called:

Master of the SOC

In this activity, you will work in groups of three or four as SOC analysts.

Part 1 — Create Your SOC

- You will be provided logs of typical business activity for a fictional organization.
- You must analyze these logs and use them to create reports, alerts, and dashboards.

Part 2 — Protect Your SOC

- You will be provided multiple logs containing suspicious activity.
- You must use the monitoring tools created in Part 1 to analyze and protect your organization from potential attacks.

Master of the SOC

Your groups will be acting as SOC analysts at a small company called Virtual Space Industries (VSI).

- VSI specializes in the design of virtual reality programs for businesses.
- VSI has heard rumors that a competitor, JobeCorp, may be planning cyberattacks to disrupt VSI's business.

As SOC analysts, you are tasked with using Splunk to monitor against potential attacks on your systems and applications.

Master of the SOC

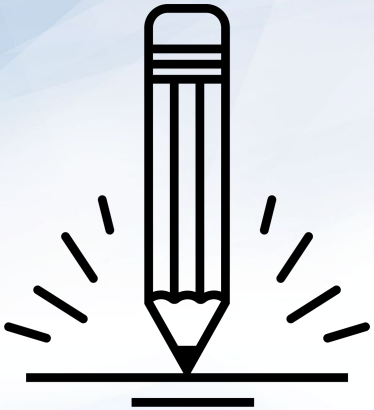
Your Networking team provided you with past logs to help you develop baselines and create reports, alerts, and dashboards.

After you design your monitoring solutions, you will use logs of attacks from JobeCorp to determine if your monitoring solutions were successful.

```
83.149.9.216 - - [17/Mar/2020:10:05:03 +0000] "GET
/presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:43 +0000] "GET
/presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:47 +0000] "GET
/presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:12 +0000] "GET
/presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:07 +0000] "GET
/presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:34 +0000] "GET
/presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```

Guidelines

- Groups will be provided two VSI logs files: a Windows server and an Apache web server.
- Use the Splunk **Search & Reporting** application.
- In each group, each individual student should be working in their own Splunk environment to conduct the activities.
- One student in each group should have the "master" Splunk SOC environment that contains all of the deliverables.
- The group must complete all deliverables. Each group decides how the SOC is designed and deliverables are achieved.
- Groups can use any resource while completing the activity: class notes, slides, Splunk online resources, etc.
- If time permits, several groups can present their SOC at the end of class.



Part 1: Create Your SOC

As SOC analysts, you are tasked with using Splunk to monitor against potential attacks on your systems and applications.

Suggested Time:
1 Hour 15 Minutes


MASTER of the
SOC
BREAK

Part 2: Defend Your SOC

VSI experienced several cyberattacks, likely from their adversary JobeCorp.

- Fortunately, your SOC team recently set up monitoring solutions to help VSI quickly identify what was attacked.
- These monitoring solutions will also help VSI create mitigation strategies to protect the organization.

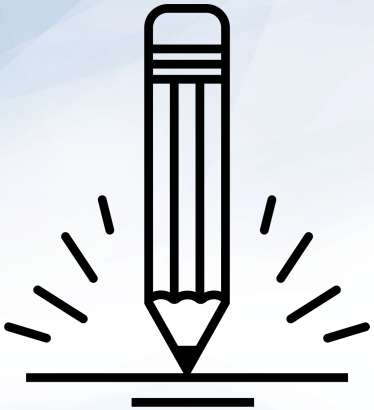
Important: One part of this activity requires particularly close attention.

Part 2: Defend Your SOC

Because you are analyzing a new set of data, after the new data file is loaded, the source must be changed on the reports, alerts, and dashboards.

Detailed instructions will be provided.

```
83.149.9.216 - - [17/Mar/2020:10:05:03 +0000] "GET
/presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:43 +0000] "GET
/presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:47 +0000] "GET
/presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:12 +0000] "GET
/presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:07 +0000] "GET
/presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [17/Mar/2020:10:05:34 +0000] "GET
/presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406
"http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```



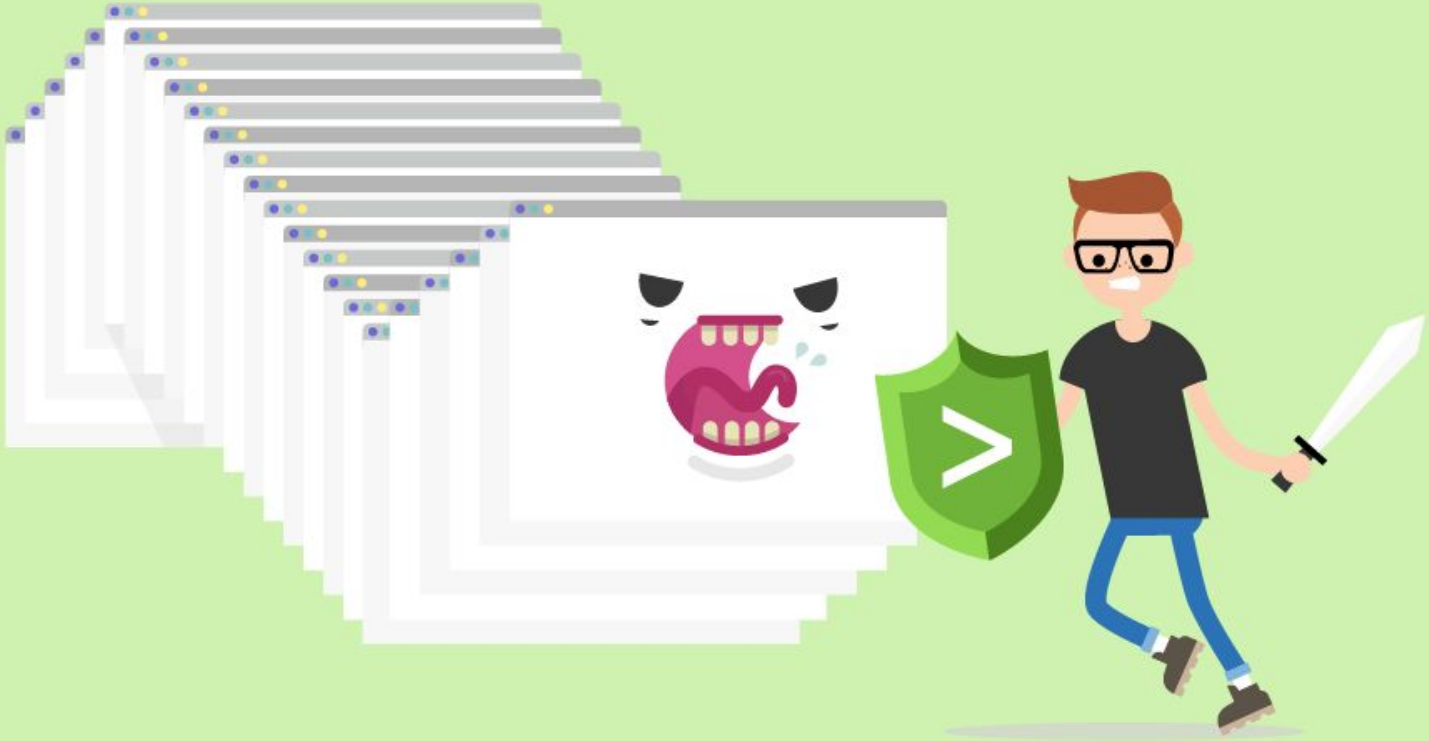
Part 2: Defend Your SOC

You will use your newly implemented monitoring solutions to help VSI quickly identify what was attacked.

Suggested Time:
1 Hour 15 Minutes

Time’s Up! Let’s Review.

This week's homework will be a continuation of today's activities, focusing on how to mitigate against the attacks you identified.




MASTER of the
SOC
Good work!