CYBERROOKIE

CYBERROOKIE

CYBERROOKIE

CyberRookie Project - Learning Cyber Skills By Building A HomeLab

Trevor Shi

CYBERROOKIE

Week 6 Lesson - Security Monitoring/SIEM

CYBERROOKIE

Overview

1. Log Event VS. Incident
2. SIEM Solution
3. Splunk SIEM
4. IBM QRadar
5. Azure Sentinel
6. ELK Stack

Log Event VS. Incident

1. **What is the Event?**
   An Event is any change, error or interruption within an IT infrastructure.
   Any observable occurrence in a system or network. - NIST

2. **What is the Incident?**

   An Adverse event that negatively impacts the confidentiality, integrity and availability of data.

CYBERROOKIE

SIEM Solution

1. **What is SIEM?**
   https://www.varonis.com/blog/what-is-siem/
   https://www.imperva.com/learn/application-security/siem/

2. **Top SIEM Tools**
   Splunk
   IBM QRadar
   LogRhythm
   Azure Sentinel
   ELK Stack

CYBERROOKIE

Splunk SIEM

1. **Introduction**
   https://www.splunk.com/en_us/cyber-security/siem.html

2. **Free training Course**
   Splunk Fundamentals part 1
   https://www.splunk.com/en_us/training/free-courses/splunk-fundamentals-1.html
   # 1 month limited access, with LAB Exercises that be down on your personal PC.

3. **Free Trials and Downloads**
   https://www.splunk.com/en_us/download.html

4. **Certification Information**
   https://www.splunk.com/pdfs/training/Splunk-Certification-Candidate-Handbook.pdf

CYBERROOKIE

IBM QRadar

1. **Introduction**

   https://www.ibm.com/security/security-intelligence/qradar?p1=Search&p4=437000503703221 80&p5=e&gclsrc=aw.ds&gclid=Cj0KCQjw8vqGBhC_ARIsADMSd1CzW2JFTbDseg5taoGrM0Cjv-tASr3B0DoTsXSEwUTB7qJwuIRkhlMaAo_sEALw_wcB

2. **Training Course**

   QRadar Foundations Part 1

   https://www.youtube.com/watch?v=6u2H4BJeEns&ab_channel=%23FunnyMovement.

   https://www.securitylearningacademy.com/

3. **Free Trials and Downloads**

   IBM Security QRadar Community Edition

   https://www.ibm.com/community/qradar/ce/

CYBERROOKIE

Azure Sentinel

1. **What is Azure Sentinel?**

   Azure Sentinel documentation

   https://docs.microsoft.com/en-us/azure/sentinel/

2. **Training Course**

   Become an Azure Sentinel Ninja

   https://techcommunity.microsoft.com/t5/azure-sentinel/become-an-azure-sentinel-ninja-the-complete-level-400-training/ba-p/1246310

   Learn Azure Sentinel on Microsoft Learn

   https://techcommunity.microsoft.com/t5/itops-talk-blog/learn-azure-sentinel-on-microsoft-learn/ba-p/2006346

3. **Free Trials**

   Azure free account with 12 months of free services

   https://azure.microsoft.com/en-au/free/

CYBERROOKIE

ELK Stack

1. **Introduction**

   https://www.ibm.com/security/security-intelligence/qradar?p1=Search&p4=437000503703221 80&p5=e&gclsrc=aw.ds&gclid=Cj0KCQjw8vqGBhC_ARIsADMSd1CzW2JFTbDseg5taoGrM0Cjv-tASr3B0DoTsXSEwUTB7qJwuIRkhlMaAo_sEALw_wcB

2. **Training Course**

   Free Elastic training

   https://www.elastic.co/training/free

3. **Downloads**

   ELK Stack

   https://www.elastic.co/start?elektra=organic&storm=CLP&rogue=free-and-open-gic

CYBERROOKIE

Q&A

Look forward to your feedbacks and suggestions.
Contact: CyberRookieProject@gmail.com

CYBERROOKIE

Thank You