kaspersky.academy

Security Monitoring and Cyber Threat Hunting

Curriculum

Sergey Soldatov
Kaspersky Lab

17.06.2019

kaspersky.academy

Security Monitoring and Cyber Threat Hunting

Course Duration

44 instructor-led hours (+ 70 hours of individual study)

Abstract

Information security is a complex of processes, people, and technologies, and their mutual effectiveness defines efficiency of an overall Infosecurity program in the enterprise. "Security operations" is the crucial glue between these three components and Security operations center is its implementation in practice.

During the module classes, students get acquainted with modern attack tactics, techniques, and procedures and how they can be addressed by security operations staff. In lab classes, students will get practical skills in attack detection and investigation.

Objectives & Learning Goals

The course is designed to enable the students who pass the course do the following:

- Plan and organize security monitoring in the enterprise
- Use different threat intelligence sources to find new advanced threats
- Detect and investigate malicious activity in windows and linux infrastructures based on attacker’s TTP
- Build cyber threat hunting infrastructure based on open source solution

Methodology

Each theoretical material will be worked off on lab and homework sessions with practical exercises. The most of the practical exercises will be linked together as different chapters of a single story that allows students to learn in practice how to use various technological approaches and tools.

Evaluation and grading

Course grades will be determined using the following breakdown: lab - 40%, homework — 30%, final exam — 30%.

kaspersky.academy

Course Outline

1. **General concepts**
   - 1.1. Current state of cyber threats
   - 1.2. Operational security goals and approaches
   - 1.3. Security operations center architecture, processes and tools
     - 1.3.1. Typical SOC infrastructure
     - 1.3.2. Firewalls
     - 1.3.3. IPS/IDS
     - 1.3.4. Breach detection solutions
     - 1.3.5. SIEM-system
   - 1.4. Cyber threat intelligence (TI)
     - 1.4.1. What is TI
     - 1.4.2. Levels of TI: tactical, strategic, operational
     - 1.4.3. TI sources and methods: HUMINT, OSINT, etc.
     - 1.4.4. TI platforms
     - 1.4.5. How to use TI in security operations
   - 1.5. Cyber threat hunting
     - 1.5.1. From reactive to proactive: malware less attacks, targeted attacks, file less attacks
     - 1.5.2. David Bianco's pyramid of pain
     - 1.5.3. MITRE ATT&CK framework and Attack Kill chain
     - 1.5.4. TTP[1]-based detection approach
     - 1.5.5. Required data for threat hunting
     - 1.5.6. Threat hunting process
   - 1.6. Lab: Setting up your monitoring and hunting infrastructure based on ELK stack[2]
     - 1.6.1. What is ELK stack
     - 1.6.2. Logstash features
     - 1.6.3. KIBANA: query syntax and dashboards
     - 1.6.4. Beats

2. **Network and perimeter security**
   - 2.1. Network security architecture: segmentation, zone security, etc
   - 2.2. Network security devices: switches, routers, firewalls, NG-FW, WAF, IPS/IDS, web security gateways, e-mail security gateways, Anti-APT, DLP, honeypots/honeynets, etc
   - 2.3. Common network attacks, attack tools and network monitoring: L2 attacks, (DNS, NBNS, LLMNR)-spoofing, different scans/sweep, etc
   - 2.4. Matching IP-MAC-Switch port-username
   - 2.5. Network security monitoring (NSM) overview
     - 2.5.1. What is NSM
     - 2.5.2. NSM Data sources: Flow. Traffic, Transactions, Alerts, Correlated Alerts
     - 2.5.3. Main NSM abilities: client and server-side attack detection, files transferring tracking, command and control traffic identification, anomalies detection, network inventory.
     - 2.5.4. NSM Design and Architecture
   - 2.6. Transaction logs analysis: Proxy, Mail, DNS, Web
   - 2.7. Network IDS (NIDS): Snort, Suricata
   - 2.8. Bro Network Security Monitor
   - 2.9. Network Traffic analysis

3. **Windows**
   - 3.1. Windows architecture and security
   - 3.2. Native Windows logs and monitoring
     - 3.2.1. Advanced audit policy with Legacy audit policy

[1] Tactics, Techniques and Procedures
[2] https://www.elastic.co/webinars/introduction-elk-stack

3.2.2. Important windows events and why they are
3.2.3. Manual log analysis: Windows Event viewer, Powershell, LogParser
3.2.4. Windows event forwarding
3.3. Additional Windows log sources: Sysmon, Autoruns
3.4. Windows Post Exploitation TTP (Persistence, Privilege Escalation, Defense, Execution, etc.)
3.5. Active Directory attacks and detection (Pass-the-Hash, Overpass-the-hash, Pass-the-Tiicket, Golden Ticket, Silver Ticket, Kerberoasting)

4. Linux
4.1. Linux architecture and security
4.2. Linux logs and monitoring
4.3. Important Linux logs and what they can tell
4.4. Centralized Linux logs processing
4.5. Linux System Auditing with Auditd
4.6. Linux Post Exploitation TTP (Persistence, Privilege Escalation, Defense, etc.) and their detection

5. Other security operations tasks
5.1. Security assessment and compliance
5.2. Vulnerability management
5.3. Change management and access control

Practice Sessions

1. ELK
2. ARP poisoning
3. Bro
4. Suricata IDS
5. Server-side attack
6. Windows Security
   6.1. User rights, cleartext passwords, and hashes in the memory
   6.2. Privileges, token stealing attack, UAC
7. Windows Security Audit
   7.1. Audit policy configuration
   7.2. Forwarding events to the TELK
   7.3. Object Access Audit
   7.4. Logstash enrichment
   7.5. Manual hunting and log analysis
8. Automatic hunting using X-Pack watcher
9. Sysmon
   9.1. Deployment
   9.2. Logstash enrichment
10. Autorun, Logstash parsing and feed checking

kaspersky.academy

Bibliography

Core materials:

- Adversarial Tactics, Techniques & Common Knowledge. https://attack.mitre.org/wiki/Main_Page
- Sqrrl. Your practical guide to threat hunting. https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf
- iSight partners. Definitive guide to cyber threat intelligence. https://cryptome.org/2015/09/cti-guide.pdf
- Scott J. Roberts, Rebekah Brown. Intelligence-Driven Incident Response: Outwitting the Adversary
- Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response 1st Edition
- Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich, and David A. Solomon – Windows Internals, Seventh Edition, Part 1
- Stuart McClure, Joel Scambray, George Kurtz. Hacking exposed. Network security secrets and solutions.
- Stuart McClure, Joel Scambray. Hacking exposed. Windows

Additional materials:

- Jason T. Luttgens, Matthew Pepe, Kevin Mandia. Incident Response & Computer Forensics, Third Edition
- Ten strategies of a World-Class Cybersecurity Operations Center. https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

Prerequisites

Good knowledge of operating systems and network protocols.

kaspersky

www.kaspersky.com/
www.securelist.com

© 2019 AO Kaspersky Lab.
All rights reserved. Registered trademarks and service marks are the property of their respective owners.