GUIDEM

COURSE SYLLABUS

Cyber Defense & Threat Hunting

Practical hands-on course in order to become an effective blue teamer. This course dives deep into the process, tools, hunting mindset, tactics for triage and investigation, analyzing malicious events, and common strategies on how to perform Incident Response.

Authors: Mark Christian Secretario & Renzon Cruz

Company Profile

GuideM is a top specialized training and consulting services provider that delivers real-world approaches in both Offensive (Red) and Defensive (Blue) disciplines of Cybersecurity in the Philippines. We provide professional training and services wherein we take pride in producing world-class quality comprehensive, highly technical, and purely hands-on courses.

OUR INSTRUCTORS

- Seasoned Industry Professionals
- Several years of Experience
- Well known in the industry

OUR COURSES

- Hands-on exercises
- Real-world use cases
- Quality discussion
- Final Challenge (CTF)

GuideM Training courses are intensively for security practitioners to gain real-world hands on knowledge which aim to equip useful skills and practical knowledge that is up to date.

Our Founder

Mark Christian Secretario, also known as Ian, is a highly experienced cybersecurity professional and the esteemed founder of GuideM. Beyond his technical expertise, He plays a pivotal role in leading GuideM's training and consulting services, offering Security Assessments, VAPT, Red Team, Purple Team, and cybersecurity advisory.

Ian is also responsible for the implementation of a cutting-edge learning platform, keeping GuideM at the forefront of technological advancements. He is actively involved in the company and client's growth, personally teaching and developing both offensive and defensive cybersecurity courses, solidifying GuideM's reputation as a trusted authority in the field. He also guides clients in vetting potential employees from the talent pool and oversees immersive learning events, and customized in-house training. Additionally, Ian is working closely mentoring and guiding the next generation of cybersecurity professionals.

Course Overview

Cyber Defense & Threat Hunting course covers essential topics related to blue team security operations, incident response, and threat hunting. Various topics will be discussed that will teach you the fundamentals of proper defensive mindset, security analysis & investigation, and how to hunt advanced attacks in a corporate environment.

This course will teach you also how to perform detection engineering and methodology. You will learn different TTP based on MITRE ATT&CK and how to use this framework to map your detection capability. This course also tackles the incident response process and will perform data acquisition in a live box machine environment full of a simulated attack.

Best of all, we will cover how to detect and analyze advanced techniques from the offensive side such as offensive PowerShell attacks, File-less attacks,s and abusing Living-Off-The-Land Binaries.

Course Structure

This training course presents comprehensive cyber defense concepts as well as threat hunting capabilities that you can leverage in your current work or future career. Our topics included on this bootcamp were chosen efficiently based on the current demand of the market when looking for a rockstar cyber defender and threat hunters. The objective of this course is to strengthen your defensive mindset and hunting capability to act quickly when it comes to detection and response.

Learn Cyber Defense & Threat Hunting based on the real world scenarios and use-cases.

Training Highlights

- 25+ Hand-on Lab Activities
- 600+ Presentation Slides
- 3 Custom VMs to be given away
- Analyst VM with 300+ security tools, multiple IR playbooks, sample Intel Reports, etc
- Malicious VM to practice Incident Response and Investigation
- Hunting VM with more than 15 threat hunting use cases
- Final Hunt The Kingdom challenge (CTF)
- GuideM Certification Exam:
  Certified Defense Analyst (CDA)

Course Author

RENZON CRUZ | @r3nzsec

GCTI | GREM | GDAT | GNFA | GCFA | GCFE | GCIH | eCTHP | eCDFP | eJPT | MCS | MCP | ITIL

Co-Founder of GuideM | Principal Consultant - DFIR @ Unit 42 Palo Alto Networks

- 11 yrs. of Cybersecurity experience
- Ex-Senior Security Consultant for National Security - GCC
- Member of TheDFIRReport & HackStreetBoys PH CTF Team
- Course Author & Lead Instructor for DFIR/Cyber Defense/TH

Specialties & Focus Area:

- SOC & Threat Hunting/Detection Engineering
- Digital Forensics & Incident Response (DFIR)
- Malware Analysis & Reverse Engineering
- Adversary Simulation & Purple Teaming

Speakership:

- BSides London 2019, UK
- BSides Vancouver 2019, Canada
- BSides Doha 2020, Qatar
- ROOTCON PH 2020, Philippines
- NorthSec 2021, Montreal
- DEFCON 2021, USA Las Vegas - Blue Team Village
- IWCON 2023 - India (Online)

Certifications:

- GIAC Certified Threat Intelligence (GCTI)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Certified Forensics Analyst (GCFA)
- GIAC Network Forensic Analyst (GNFA)
- GIAC Defending Advanced Threats (GDAT)
- GIAC Certified Forensics Examiner (GCFE)
- GIAC Certified Incident Handler (GCIH)
- eLearnSecurity Threat Hunting Professional (eCTHP)
- eLearnSecurity Digital Forensics Professional (eCDFP)
- eLearnSecurity Junior Penetration Tester (eJPT)

GUIDEM

Course Author

MARK CHRISTIAN SECRETARIO | @iansecretario_

Red Team Consultant / Penetration Tester

11+ years in Information Technology

- Malware Development & Purple Team Practitioner
- Freelance & Independent Consultant

Founder and Lead Instructor

- Cybersecurity Training & Services Provider

Hackstreetboys Member

- All Filipino CTF Team

Specialties & Focus Area:

- Red Team/Offensive Security
- Purple Team/Adversary Simulation
- Security Research & Exploit Development
- Evasion and Malware development

Certifications:

- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Enterprise Vulnerability Assessor (GEVA)
- GIAC Exploit Researcher & Advanced Penetration Tester (GXPN)
- GIAC Web Application Penetration Tester (GWAPT)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional(OSCP)
- Certified Red Team Professional (CRTP)
- Certified Red Team Expert (CRTE)
- Certified Red Team Operator(CRTO)
- Certified Red Team Master(CRTM)
- Certified Red Team Lead(CRTL)
- Certified Azure Red Team Professional (CARTP)
- Red Team Operator Level 1 – Rastalabs (Hackthebox)
- Red Team Operator Level 2 – Cybernetics (Hackthebox)
- Red Team Operator Level 3 – APT Labs(Hackthebox)
- Elearnsecurity Exploit Development Professional(eCXD)
- Elearnsecurity Certified Penetration Testing Extreme(eCPTXv2)
- eLearnSecurity Web Application Penetration Tester Expert (eWPTX)
- eLearnSecurity Web ApplicationPenetration Tester (eWPT)
- Pentester Academy Certified Enterprise Specialist (PACES)
- Certified Red Team Professional (Cyberwarfare)
- Certified Red Team Analyst (CyberWarfare)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Network Associate (CCNA)
- CCNA Cyber OPS

Course Information

System Requirements

- Core i5/Ryzen 5 or greater
- 8GB RAM minimum
- 100GB free storage
- Installed Virtualization software such as VMware Workstation or Fusion

Target Audience

Cyber Defense & Threat Hunting Bootcamp focuses on defensive strategies normally done by existing SOC Analysts. If you want to improve your skills in terms of Incident Response & Threat Hunting aside from doing the usual threat monitoring, this course is for you.

Blue Team / IT Security Professionals

- Aspiring SOC Analyst | Incident Responder | Threat Hunters
- Career shifters such as Software Engineer, HelpDesk, Network Engineer, System Administrator, etc.
- IT Professionals with a minimum of 1-2 yrs of related experience

Red Team / Penetration Testers

- Penetration Tester who wants to know how detection works and to improve their evasion techniques

GUIDEM

MODULE 1

Introduction to Blue Team

This module will equip the student with the fundamentals of the blue team, identify the mission of a SOC and how to understand an organization's threat model. They will also learn the different roles in a SOC, functions and capabilities to become an effective Security Operations Center Analyst. We will also cover some of the frameworks being used by most companies that have a security team on their belt. Students will also learn the common Open Source Intelligence tools that we can leverage on a daily basis when performing a SOC role. We will also discuss some of the famous APT groups, how their methods differ and lastly, their motivations.

Topics

- Blue Team Overview
- SOC Overview I Different Roles In SOC
- A Day in the Life of a SOC Analyst
- Security Analyst Toolset (Open Source)
- Events, Alerts and Incidents
- Pyramid of Pain
- Tools in SOC (Enterprise I Open Source)
- Malware Fundamentals & Triage for SOC
- Networking Fundamentals & Analysis Toolkits
- Security Framework Overview

Hands-on Exercises

- SOC Alert Analysis & Triage
- Malware Static Analysis using PEStudio, CAPA & CFF Explorer
- Malware Investigation using FLOSS String Extraction
- Malware Dynamic Analysis using Sysinternals
- Analyze Network PCAP using WireShark and BruteShark
- Unveiling Network Mysteries: PCAP Analysis with NetworkMiner
- Network Analysis using BRIM

MODULE 2

Introduction to Incident Handling

This module covers a lot of incident handling procedures, workflow, standards and tools. The student will be introduced to the Incident Handling Process in detail.

We will also cover the cyber kill chain and how to prepare and defend against each stage. Our goal is to educate each student on the TTP (techniques, tactics and procedures) that modern adversaries use in order for them to become prepared and defend against it.

We also have a collection of scripts/tools that we use to collect and gather data when Incident Responder kicks in. Usage of these scripts/tools will be discussed alongside when performing the lab exercise.

Topics

- Introduction to Incident Handling
- Threat Intel Led Incident Response
- Long Tail Analysis in IR
- Data Acquisition Process
- Key Windows Artifacts for Incident Response
- Cyber Kill Chain (Attack & Defend)
- IR Run Books & Workflow
- Open Source Tools - Scripts for IR
- Real-World IR Engagements & Lessons Learned

Hands-on Exercises

- Enterprise IR - Initial Access, Identification & Analysis
- Leveraging Threat Intelligence & OSINT during Incident Response
- Long Tail Analysis using PowerShell
- Data Acquisition - Live Response Collection
- Incident Response - Detecting Host Fileless Attacks

MODULE 3

Security Investigation and Analysis

In this module, students will learn how to investigate an incident or an alert. We will cover various topics and witness how common protocol analytics can greatly increase one's network visibility in attempt to detect abnormal and probably malicious actions. The student will see how they can extract actionable intrusion related information by performing SMTP, DNS and HTTP/s analytics.

We will also cover different tools on how to investigate a suspicious file. The student will learn the fundamentals of windows logging including additional auditing in windows environment (Account Management, Auditing Power Shell, Logon Events, Scheduled Task Logging, etc.). The student will also learn the top security event IDs that are commonly being monitored by SOC teams to identify suspicious behavior.

Topics

- Detecting Malware Persistence
- Endpoint Analytics
- Tools for Investigation
- PDF/MS Office Malicious Files Investigation
- Spot the Adversary w/ Windows Event IDs
- Best Practices of Windows Logging

Hands-on Exercises

- Intrusion Analysis: Persistence Techniques
- Live System Investigation
- Maldocs Analysis (Word Document & PDF)
- Maldocs Analysis - Malicious Macros in Excel
- Live System Investigation - Malicious Windows Machine
- Rapid IR Investigation - Malicious Windows Machine

MODULE 4

Introduction to Threat Hunting

Student will be introduced to the world of threat hunting which will include a brief of what threat hunting is and why companies seek to establish this capability within their organization. Hunting mindset will be covered wherein the student will either lean on towards threat intel or DFIR.

We will also dive in to the world of Windows Internals where the student will learn how to detect what is normal or potentially malicious. We will also show how to detect famous offensive tools being used by Red Teamers or possibly threat actors such as Mimikatz, Malicious Macros, Code Injection and many more using the capability of Sysmon. Also, not limited to only endpoint analysis, we will also include how to recognize normal network traffic and how to detect network traffic patterns. Not familiar with MITRE ATT&CK Framework? We got you covered. Not only that, we will also tackle the SIGMA Rules for SIEM Systems and discuss some of the successful detection strategies.

Topics

- Threat Hunting Methodology
- MITRE Framework (ATT&CK)
- Sigma Rules for SIEM Systems
- What to Hunt? (Network, Endpoint)
- Data Stacking - TTPs & Behavior
- Windows Processes (Core)
- All About SYSMON
- Analyzing Windows Event Logs
- Real World Scenario & Use Cases

Hands-on Exercises

- Accessing ELK thru Local Browser
- Threat Hunting: Introduction to ELK & Visualization
- Threat Hunting: Credentials Attack
- Threat Hunting: Log Tampering, C2 IP and Petya Ransomware
- Threat Hunting: PUP, Phishing Attack and Ransomware Artifacts
- Threat Hunting: Detection Engineering
- Windows Event Logs vs SYSMON

MODULE 5

Practical Threat Hunting

For the last module, we will focus more on hands-on activities thru analysis and hunting suspicious activities. We will provide a custom VM and some PCAP files for the student's network hunting activity. We will also deal with IOCs and how to manage bulk IOCs using an open source tool. We will also cover the most common attack nowadays used by adversaries based from Red Canary survey of this year, Offensive PowerShell. On this topic, we will show the student the most common arguments in PowerShell that can be abused by threat actors and how to detect this attack as well. After the discussion, students will be able to play our very own "Hunt The Kingdom" capture the flag competition.

Topics

- Offensive PowerShell & How to Detect it
- Managing IOCs
- Hunting Malware
- Malware Sandbox (Online Resources)
- Hunt the Kingdom (CTF)

Hands-on Exercises

- Hunt the Kingdom (CTF Style)

Contact Us

training@guidem.ph

facebook.com/guidemtraining

linkedin.com/company/guidemtraining

twitter.com/guidemtraining

instagram.com/guidemtraining

GUIDEM