PurpleLABS Training Portfolio 2022

Defensive Security delivers high-quality cyber security services including Linux / Windows digital forensics, incident response, latest threat analysis, and hunting, penetration testing, and infrastructure hardening. We successfully deliver a combination of Threat / Adversary Emulations vs network / endpoint investigations and log analysis at scale which is known as Purple Teaming.

We offer advanced, hands-on cyber security training programs backed by PurpleLabs - a fully customized Cyber Range Environment enriched by step-by-step offensive / defensive hands-on lab instructions. Want to sharpen your Purple team skills? Try dedicated PurpleLabs training programs:

1. Adversary Emulation and Breach Attack Simulations
2. C2 Matrix Operator → Post-Exploitation and Evasion Techniques
3. Advanced Network Detection and Threat Hunting
4. Linux Forensics Inspection and Incident Response at scale
5. Windows Forensics Inspection and Incident Response at scale
6. Advanced Linux Security and Hardening

Adversary Emulation and Breach Attack Simulations

Adversary emulation is a type of red team engagement that mimics a known threat to an organization by blending in threat intelligence to define what actions and behaviors the red team uses. This is what makes adversary emulation different from penetration testing and other forms of red teaming. Adversary emulators construct a scenario to test certain aspects of an adversary's tactics, techniques, and procedures (TTPs). The red team then follows the scenario while operating on a target network in order to test how defenses might fare against the emulated adversary.

Breach and Attack Emulation solutions allow you to continuously assess risk posture and exposure to attacks in modern network environments. The validation of the detection coverage has become one of the key responsibilities of SOC team members.

Attack Emulation tools allow you to safely create and run dedicated real-world adversary campaigns at scale by mimicking different phases of attack and mapping them to MITRE ATT&CK Framework:

- Initial Access Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

Attackers constantly find new ways to attack and infect Linux / Windows networks using more and more sophisticated techniques and tools. As defenders we need to stay up to date with adversaries, understand their TTPs, be able to respond quickly and repeat their actions on demand. As SUN TZU said: "To know your enemy, you must become your enemy" and this is the main goal of this Purple-team oriented Adversary Emulation training.

This training program is about monitoring and measuring security controls by executing (semi-) automated scripted attacks. Every single emulation job or tool in use will be well-described and analyzed in terms of their nature and detection scopes including TTP's artifacts and behaviors which we are going to hunt for using live PurpleLabs Cyber Range telemetry and analytics including Sysmon, Windows Event Logs, Zeek IDS, Suricata IDS, Moloch FPC, Elastiflow, Velociraptor, OSquery, Sigma rules, Splunk, Hunting ELK and more.

Through the hands-on labs you will be playing with a variety of emulation scenarios based on:

- PurpleSharp / PurpleAD
- Atomic Red Team
- Caldera
- Infection Monkey
- APTSimulator
- Metta
- AutoTTP
- ATTPwn
- DumpsterFire
- Purple Metasploit
- TestMyNIDS
- PyExfil
- FlightSim
- RTA
- GoPurple
- Covenant
- Empire
- Sliver
- Vectr, Unfetter and many more

Different ways of automation and customization will be presented as well.

At the end of this class you will understand the value of the Assume Breach approach and the business need for emulation of threats after getting early access (C2, Lateral Movement, Persistence, Evasion). You will gain the knowledge and tools to begin executing assumed-breached, chained attack paths. You will get knowledge also about important Open Source defensive security stack and visibility needs within your environment at many different levels.

In terms of data leakage protection and for better understanding a current status of your network security posture, this training helps you identify risks, network security blind spots, issues with event logging pipeline and unexpected and uncovered areas by emulating a real cyber adversary behavior.

Agenda / what you will learn:

- Introduction to Adversary Emulation, BAS solutions and Purple Teaming:
    - The Build / Attack / Defend Pyramid

- MITRE Attack Framework → The industry standard and common language between Blue Teams, Red Teams and CTI

- The overview of Security Control Framework Mappings
- Visibility is the key → Open Source Defensive Security Stack for Blue / Threat Hunting Team:
    - Sysmon
    - Windows Event Logs
    - Zeek IDS
    - Suricata IDS
    - Moloch FPC
    - Velociraptor DFIR
    - Wazuh
    - Netflow Elastiflow
    - OSquery
    - Splunk
    - Hunting ELK
    - Strelka
    - Sigma rules

- Atomic Red Team tests at scale vs detection
- PurpleSharp architecture and advanced simulation playbooks in Active Directory
- Caldera architecture, plugins overview and APT-based evaluation scenarios:
    - FIN6
    - APT28
    - APT29
    - APT41
    - FIN7
    - menuPass
    - Hafnium
    - Carbanak
    - and more

- Egress testing, C2 channels and suspicious network events vs detection
- Playing with various Windows / Linux shellcode injection techniques vs detection
- Hands-on analysis and activity replication of the latest APT groups
- Integration and automation of emulation arsenal tools
- Challenge - create your own APT emulation scenario + detection/hunting

---

Target Audience:

- CSIRT / Incident Response Specialists

- Red and Blue team members
- Penetration testers
- Threat Hunters
- Security / Data Analytics
- IT Security Professionals, Experts & Consultants
- SOC Analysts and SIEM Engineers
- AI / Machine Learning Developers
- Open Source Security Enthusiasts

C2 Matrix Operator: Post-Exploitation & Evasion Techniques

There is a huge opportunity for defenders to understand the spectrum of offensive capabilities, behaviors, generated IoC's and leftover artifacts of modern C2 Frameworks execution. Knowing your enemy is critical. Simultaneously, attackers do the same exercise, but in the opposite direction.They analyze detection capabilities of blue team tools against their C2 / post-exploitation arsenal tooling. Based on that, adversaries constantly find new evasion techniques to stay hidden and undetected during post-exploitation activities. And again, defenders should continue doing offensive research to stay updated and gain better detection coverage.

This hands-on training will introduce students to the world of C2 Frameworks and related offensive projects, their functionalities, post-exploitation modules, different kinds of network communication channels, extensions and chaining capabilities. We will go through different programming languages to achieve the attacker's goals. Expect C2 customization, generating undetected loaders and payloads, using obfuscation methods, in-memory payload execution, domain fronting, redirectors, UAC / AMSI / Defender bypassing just to name a few.

Each of the steps: enumeration, privilege escalation, persistence, pivoting and lateral movement will be covered as hands-on instructions compatible with PurpleLabs - a cloud based Cyber Range Playground that includes:

- Sysmon
- Windows Event Logs
- Zeek IDS
- Suricata IDS
- Moloch FPC
- Netflow ElastiFlow
- Velociraptor DFIR
- Falco
- Wazuh
- OSquery
- Splunk
- Hunting ELK
- Sigma rules

Saying that, in addition to the offensive part, you will have the opportunity to run hunting and detection activities, thus achieving a bigger picture about adversary tradecraft.

Highly technical content and only a hands-on practical approach guarantees that the usage of this transferred knowledge in real production environments will be easy, smooth and repeatable.

Training description in keywords:

Sliver, Covenant, Mythic, Empire, PoshC2, Koadic, C3, Metasploit, Octopus, DNSStager, Singularity, Faction, Puppy, DET, ChunkyTuna, EvilRM, SilentTrinity, sg1, TrevorC2, Weasel, ngrok, shadowC2, pspy, pupy, Cobalt Strike, goDoH, Merlin, NinjaC2, SharpC2, ThunderShell and more.

Agenda / what you will learn:

- Introduction to C2 Matrix
- Current state of APT campaigns in terms of popular C2 usage
- Distributed / multi-node C2 Architectures
- Staging / stageless payloads
- Generating different types of implants and in-memory execution of VBScript, JScript, EXE, DLL files and dotNET assemblies
- Implants execution in different formats: HTA, MSI, JS, VBS, WSF, ZipExec, ISO, binjection
- Beacon intervals, jitter, padding and expiration/kill dates
- Malleable C2 profiles / Blending into the normal traffic
- Cloning and armoring popular websites
- CDN domain fronting for C2
- Domain categorization for C2
- LOLbins / one-liners for TCP/UDP bind, reverse shells and data transfer
- SSH Tunneling, SMB pivoting, Socat relaying, IPtables port forwarding HTTP and proxying
- Execute-shellcode, execute-assembly
- Process migration and different types of process / shellcode injections
- C2 extensions loading and tooling customizations
- Dumping credentials at scale and user impersonation
- ICMP C2 and exfiltration
- C2 over HTTP/1.1, HTTP/2, and HTTP/3 protocols
- Webshells as SOCKS proxy
- DNS Tunneling / DNS-over-HTTPS C2 and payload delivery
- Pwning Docker API over DNS Rebinding
- P2P Named pipe C2
- AD / LDAP as hidden storage

- Outlook as C2
- Word / Excel document weaponization
- Browser pivoting
- Data exfiltration using X509 digital certificates
- mTLS/SSL-based C2 communication channels
- VPN-based C2 communication channels
- Cloud-based exfiltration techniques and C2 channels:
    - Slack as C2
    - SSH over Google Drive
    - Pastebin as C2
    - Youtube Comments as payload delivery channel
    - Telegram as C2
    - Discord as C2
- Lateral movement over psexec, atexec, wmiexec, dcomexec
- Active Directory enumeration methods: RPC / LDAP
- Active Directory and Kerberos attacks:
    - Golden Tickets
    - Silver Tickets
    - Kerberoasting
    - Pass The Hash
    - Pass The Ticket
    - DCSync
    - Skeleton Key
    - Password spraying
    - NTLM Relay to AD CS

- Bypassing UAC
- Evading AV/EDR by using direct system calls
- BloodHound - attack paths visualization
- Playing with different persistence methods (user space / kernel space)
- Hunting laterally for data
- Securing your C2 infrastructure (FW, port-knocking, WAF)

Target Audience:

- CSIRT / Incident Response Specialists / Threat Hunters
- Red and Blue team members
- Penetration testers
- Security / Data Analytics Engineers
- IT Security Professionals, Experts & Consultants
- SOC Analysts and SIEM Engineers
- AI / Machine Learning Developers

Advanced Network Detection and Threat Hunting

The main goal of this training is to show by hands-on the “Feel the network” approach to better understand what is normal activity, what is malicious and thus how to do incident response faster and more precisely. During this training you will analyze different types of PCAPs and live network communication streams between endpoints.

We will start by analyzing and creating a current-state behavior profile for a small network segment consisting of Linux and Windows stations. Then, we will execute various types of network attacks including lateral movement, pivoting and C2 communication channels in order to generate suspicious events. During the next step, you will identify systems that have been compromised and run a drill-down analysis.

On top of that you will spend most of your time analyzing and pivoting through available network telemetry including Netflow, Moloch as a Full Packet Capture engine, signature-based Suricata IDS and signature-less Zeek event logs like: conn.log, dns.log, dhcp.log, ssh.log. x509.log, ssl.log, ntlm.log, kerberos.log, ntp.log, weird.log, notice.log, http.log, smb.log, smb_files.log, dce_rpc.log, rdp.log, known_hosts.log, dpd.log, known_services.log, known_certs. The rest of the analyzed examples will be based on the use of the great Velociraptor DFIR to pivot to the forensic phase.

We will also cover how to extend the visibility of the Zeek engine, how to create and load additional scripts, how to write your own Suricata rule, and how to pivot across different data sources. This training will guide you through threat hunting methodologies, different network attack-detection-inspection-response use-cases and NIDS architectures to teach critical aspects of how to handle network detection and Threat hunting properly at scale. Expect to build a simple Threat Hunting Playbook at the end of the training.

Training description in keywords:

Zeek, Suricata, Moloch, Splunk, Velociraptor, Netflow, Jupyter Notebooks, Kestler, PCAP-Attacks, CyberChef, HELK, Wazuh, OSquery, Falco, Sysmon, eBPF, theHive, Wireshark, Sigma rules and more.

Agenda / what you will learn:

- Introduction to Threat Hunting:
    - Intel-based hunting

    - Hypotheses-based hunting (Analytics-driven, Intelligence-driven, Situational-awareness driven)
    - Hybrid hunting

- OODA mindset
- Know your environment:
    - the importance of network baselining
    - Identification of high value users and assets

- Overview of available network telemetry and hunting tools in PurpleLabs:
    - Network
    - Endpoint
    - Pivoting to forensic phase with Velociraptor DFIR

- Network-process context is the key
- Generating Hunting Hypotheses in the scope of:
    - Initial Access
    - Execution
    - Persistence
    - Privilege Escalation
    - Defense Evasion
    - Credential Access
    - Discovery
    - Lateral Movement
    - Collection
    - Command and Control
    - Exfiltration
    - Impact

- Auditing ingress / egress traffic
- Searching for Known Indicators of Compromise / Attack (IoC / IoA)
- Hunting using network signatures:
    - ET Open Rules
    - Talos rules

- Hunting for beacons - regular activity patterns
- Detecting ICMP C2 channel
- DNS analytics / Domain Generation Algorithm (DGA) Detection & Analysis
- HTTP / HTTPS Malleable profile analysis and detection
- Anomaly Detection in HTTP / Proxy Logs
- Proxying identification
- File extraction from PCAP and network streams
- Brute-force, password spraying detection
- Lateral Movement Detections:

    - SMB Traffic Analysis
    - RPC Traffic Analysis
    - RDP Traffic Analysis
    - SSH Traffic Analysis

- Fingerprinting with JA3, JARM and HASSH
- LLMNR, NBT-NS, MDNS poisoning detection
- Detection of VPN-based C2 channels
- Detection of blockchain-based C2 channels
- Hunting for exfiltration behaviors → download/upload ratio, packet / bytes statistics, chunking detection

- Hunting enrichment with:
    - GeoIP / ASN
    - Greynoise
    - Hybrid Analysis
    - VirusTotal

- Constructing hunt flows with Kestler and Jupyter Notebooks
- Playing with Attack PCAP analysis
- Hunting for suspicious network events with RITA
- Development of Suricata rule
- Expanding Zeek visibility
- Using theHive for threat hunting and incident management

Target Audience:

- CSIRT / Incident Response Specialists
- Red and Blue team members
- Penetration testers
- Threat Hunters
- Security / Data Analytics
- IT Security Professionals, Experts & Consultants
- SOC Analysts and SIEM Engineers
- AI / Machine Learning Developers
- Open Source Security Enthusiasts

Windows Forensics Inspection and Incident Response at scale

Attackers constantly find new ways to attack and infect Windows boxes using more and more sophisticated techniques and tools. As defenders we need to stay up to date with adversaries, understand their TTPs and be able to respond quickly. The combination of low-level network and endpoint visibility is crucial to achieve that goal. For DFIR needs we could go even further with proactive forensics inspections. This training will guide you through different attack-detection-inspection-response use-cases and teach critical aspects of how to handle Windows incidents properly. Going through the hands-on labs, you will gain a perfect understanding of important DFIR Windows/Network internals and investigation steps needed to get the full picture of post-exploitation activities and artifacts they leave behind. At scale.

Training description in keywords:

Velociraptor, OSquery, Splunk, Yara, Falco, Sysmon, syslog, auditd, eBPF, Zeek, Suricata, Moloch, theHive, Plaso, Timesketch, CyberChef, Volatility Framework, DeepBlueCLI, Wireshark, Chainsaw, Zircolite, Sigma rules and more.

Agenda / what you will learn:

- How to run DFIR tasks at scale across many endpoints
- RE&CT Enterprise Matrix
- The importance of timeline analysis
- Privileged user and group enumeration
- Identification of logged users
- Interactive Triage
- Searching for files, searching for IoC (URLS, IP, signatures, patterns, CC data)
- Web browsers history analysis
- Establish a baseline for different OS components (system32 file hashing, shim cache / amcache / SRUM DB, BAM records, ACLs, running services, run/runonce keys, scheduled tasks, autoexec, envs, VSS)
- Detecting capabilities in PE, shellcode files
- Analyzing process memory regions (loaded DLLs / .NET assemblies per process)
- Process call chains / pstree / process arguments
- IMPHashing
- Detecting suspicious child processes of wmi, psexec, smbexec

- Prefetch analysis
- Timestomping detection
- Finding LNK files
- Recovering deleted files from directory
- Playing with USN.journal
- Searching in MFT for exploitation attempts
- Open source ways for memory acquisition and memory forensics
- Filesystem and process memory yara scans
- Finding and analyzing Office documents with macros
- Checking Windows Event Logs / EVTX with Sigma detection rules
- Registry modification events HKCU / HKLM
- Detecting mutants / named mutex
- Raw NTFS parsing / ADS
- Detecting parent-process spoofing
- Data correlation and hunting for suspicious network events + RITA
- Finding and analyzing Office documents with macros enabled
- Searching for persistence methods in use
- Direct interaction with endpoint: command execution on demand, system modification and quarantine examples
- Hunts enrichment and pivoting between data sources
- Playing with offline Mordor Datasets / EVTX-Attack-Samples
- Using theHive for incident management

Target Audience:

- CSIRT / Incident Response Specialists
- Red and Blue team members
- Penetration testers
- Threat Hunters
- Security / Data Analytics
- IT Security Professionals, Experts & Consultants
- SOC Analysts and SIEM Engineers
- AI / Machine Learning Developers
- Open Source Security Enthusiasts

Linux Forensics Inspection and Incident Response at scale

Attackers constantly find new ways to attack and infect Linux boxes using more and more sophisticated techniques and tools. As defenders we need to stay up to date with adversaries, understand their TTPs and be able to respond quickly. The combination of low-level network and endpoint visibility is crucial to achieve that goal. For DFIR needs we could go even further with proactive forensics inspections. This training will guide you through different attack-detection-inspection-response use-cases and teach critical aspects of how to handle Linux incidents properly. Through the hands-on labs, you will gain a perfect understanding of important DFIR Linux/Network internals and investigation steps needed to get the full picture of post-exploitation activities and artifacts they leave behind. At scale.

Training description in keywords:

Velociraptor, OSquery, Wazuh, Splunk, Yara, Falco, Sysmon, syslog, auditd, eBPF, Zeek, Suricata, Moloch, theHive, Plaso, Timesketch, CyberChef, Volatility Framework, Wireshark Cat-scale, Sigma rules and more.

Agenda / what you will learn:

- How to run DFIR tasks at scale across many Linux endpoints
- Recent Linux APT analysis
- RE&CT Enterprise Matrix
- The importance of timeline analysis and NTP synchronization
- Triage / collecting artifacts
- Privileged user and group enumeration
- Identification of logged accounts
- Searching for files at scale
- Establishing a baseline for different OS components (cron, at, rc.local, ACLs, hosts, resolv.conf, SELinux, filesystem hashing, packages and checksums)
- Process call chains / pstree / process arguments
- Collecting and analyzing important process data (/proc)
- Finding hidden processes, network connections and kernel modules
- Detecting capabilities in ELF, shellcode files
- Detecting loaded shared libraries per process
- Detecting web shells / file create notifications

- Hunting for packers, extracting binary versions and exports
- Searching for exploitation attempts in logs
- Hunting for Linux rootkits (user space / kernel space)
- Hunting for artifacts of process injection techniques
- Sysmon Events + Sigma detection rules
- Runtime Security (Falco, Tracee)
- Open source ways for memory acquisition and memory forensics
- Creating Volatility profiles
- Filesystem and process memory yara scans
- Endpoint data correlation and hunting for suspicious network events
- Network visibility with / without signature rules
- Searching for persistence methods in use
- Data correlation and hunting for suspicious network events + RITA
- Direct interaction with endpoint: command execution on demand, system modification and quarantine examples
- Hunts enrichment
- Using theHive for incident management

Target Audience:

- CSIRT / Incident Response Specialists
- Red and Blue team members
- Penetration testers
- Threat Hunters
- Security / Data Analytics
- IT Security Professionals, Experts & Consultants
- SOC Analysts and SIEM Engineers
- AI / Machine Learning Developers
- Open Source Security Enthusiasts

Advanced Linux Security and Hardening

Advanced Linux Security & Hardening is a dedicated training program about a solid base of security hardening measures powered by practical step-by-step instructions for building your own hardened systems and services. Mandatory Access Control, sandboxing, syscall auditing, binary hardening, root user limitation, low-level accountability, ACL, service isolation on different layers like seccomp, capabilities or SELinux are just the beginning of the fun.

During dedicated labs, you will find out how to use different offensive and defensive tools, scripts, and techniques to better understand how an attacker thinks and what are the critical behaviours of a modern adversary. On top of that you will explore how to design secure, hardened systems, applications and network services. Training content in Purple teaming style of “attack vs detection” will help you understand risks, identify network security blind spots and unexpected, uncovered spaces inside an OS.

This training is intended to increase skills needed to ensure data integrity on a critical system for organizations with the highest security standards. The discussed methods of automation will support the process of achieving compliance.

Key Learning Objectives / How to:

- Prepare hardened OS configuration templates and automate deployment process
- Analyzing kernel and user space exploit techniques, critical CVE, security bugs and misconfigurations from recent years
- Demonstrate that OS configuration meets security policy requirements
- Run local and network-based vulnerability scanning / CVE tracking
- Errata / security package management
- Configure Access Control Lists and special permissions, bits and secure flags
- Manage users and password policy
- Privileged and unprivileged access accounting / session recording
- Deploy basic Linux Domain Controller with SUDO / HBAC
- Understand system auditing and syscall behavioral profiling
- Manage and configure secure virtualization and Docker containers environment
- Configure and tweak targeted SELinux policy against latest exploits
- Play with Linux Kernel Runtime Guard (LKRG) vs kernel exploits
- Understand different layers for user and service isolation
- Deploy advanced network firewall rules with anti-flooding capabilities
- Run memory acquisition and deliver memory forensics actions against Linux malware
- Compile code and run binaries in a hardened way vs local privilege escalation

techniques
- Deploy Linux Bastion host

Agenda / what you will learn:

- Introduction:
    - Defense in depth
    - DevSecOps methodology
    - Threat hunting
    - NIST / STIG / CIS benchmarks
    - MITRE ATT&CK Framework

- Current state of Linux malware / APT campaigns:
    - User space rootkits:
    - Kernel space rootkits

- Discretionary Access Control (DAC) vs Mandatory Access Control (MAC)
- Secure file system design:
    - Attributes
    - Flags
    - ACL
    - FS encryption
    - Hardlinks & Symlinks

- Local and network-based vulnerability scanning / CVE tracking at scale:
    - Host
    - Container

- Local and external enumeration and reconnaissance tactics
- Hardened binaries:
    - SSP
    - NX
    - PIE
    - RELRO
    - ASLR

- The importance of SELinux:
    - Targeted policy vs exploits
    - Multi Category Security (MCS)
    - Rule Based Access Control
    - sVirt

- Linux capabilities vs SUID attacks
- $PATH Hijacking
- Restricted shells + PAM
- System call restriction - seccomp-BPF vs exploits
- In-memory process execution
- Shared library injection
- Chroot / jail / nsjail vs escaping
- Linux Containers - Docker security vs escaping
- LKM-off / ptrace-yama / and other important sysctl enforcing options
- Debuggers and profilers:
    - gdb
    - strace
    - ltrace
    - ldd
    - yara

- Behavioral analysis and hacker's fishing:
    - systemtap
    - eBPF
    - sysdig

- Integrity checking - IMA/EVM
- Grub and secure boot configuration
- Linux Domain Controller:
    - HBAC
    - SUDO
    - RBAC

- File Access Policy Daemon
- PAM configuration: 2FA / sudo_pair / time-based access
- Secure SSH / SCP / SFTP + tips and tricks
- NFS (In)Security
- Advanced network packet filtering:
    - iptables / nftables / ebtables
    - TOR detection, ipsets, IP reputation, port knocking

- Linux visibility, auditing & accounting:
    - auditd
    - syslog
    - OSSEC
    - OSquery
    - Falco
    - Tracee

- Memory forensics - Volatility Framework vs Linux malware.
- Automation of STIG Hardening standard by using:
    - Ansible roles
    - Puppet manifests
    - Chef cookbooks

- Summary and final lab.

Target Audience

- Linux Administrators / System Architects and Engineers
- DevOps / Sysops / DevSecOps Team Members
- System Architects
- Penetration testers
- IT Security Professionals, Experts & Consultants
- Open Source Security Enthusiasts

PurpleLabs Values

This training is based on the PurpleLabs Cyber Range Playground. It's a dedicated, virtual infrastructure for detecting and analyzing the behavior of attackers in terms of the techniques, tactics, procedures, and used offensive tools. The environment is to serve the continuous improvement of competences in the field of threat hunting and learning about current trends from offensive scope (red-teaming) vs direct detection perspective (blue-teaming) and DFIR. By providing high-quality training materials with the lab environment in a scalable online format, we want to enable businesses to improve the detection capacity of their SOC teams and achieve better visibility and resistance to attacks. Having hands dirty with PurpleLabs will allow you to:

- Develop the team's analytical skills required to work in the Security Operation Center environment

- Increase awareness of the complexity and dependencies between the elements of the APT campaigns, malware and the areas of detection

- Deliver a periodic knowledge transfer and systematic expansion of team competences in the field of Red + Blue = Purple teaming

- Acquire Attack Paths / Attack Lifecycles and Security Event Chains skills by combining attacker's single techniques, tactics and procedures (Chain Attack Scenarios)

- Understand the value of the Assume Breach approach and simulation of threats after early access (C2, post-exploitation, Lateral Movement, Persistence, Evasion)

- Understand what threat hunting is and why it is important
- Understand proactive DFIR and why it is important
- Acquire skills related to generating suspicious events on the layer of network and Windows and Linux operating systems and methods of their detection

- Understand the potential of Sigma rules and their values for SIEM solutions.
- Run a validation of the current security status of the organization's network and the risks involved

- Obtain knowledge on supplying/creating a complete SOC environment using Open Source software.

About Defensive Security

Defensive Security delivers high-quality cyber security services including Linux / Windows digital forensics, incident response, latest threat analysis, and hunting, penetration testing, and infrastructure hardening. We successfully deliver a combination of Threat/Adversary Emulations vs network/endpoint investigations and log analysis at scale which is known as Purple Teaming.

Defensive Security offers advanced, hands-on cyber security training programs backed by PurpleLabs - a fully customized Cyber Range Environment enriched by step-by-step offensive/defensive lab instructions. Want to sharpen your Purple team skills? Try PurpleLabs where you will be playing with chained attack paths, emulating attacker's TTPs, and running detection/response at the same time by using Sysmon and EVTX, Auditd, Wazuh, Graylog, HELK, ElastAlert, Falco, OSQuery, Velociraptor, Zeek, Suricata, Moloch FPC, Volatility Framework, theHive, MISP, and Sigma Rules.

Our mission is to help organizations have more secure infrastructures, better utilize Open Source software in Security Operations, and enable businesses to improve the detection capacity and skills of their SOC/IR teams.

We are trusted by the biggest customers from the private, oil and gas, insurance, and financial sector. It was an honor for us to conduct training workshops during the biggest conferences including Hack In The Box, BruCON, 44CON, OWASP AppSec US, and Black Hat US.

Our almost 20 years of hands-on experience with Open Source Security Solutions go directly into the full spectrum of technology solutions to support customers achieving better visibility and detections, improving offensive and defensive Red / Blue and Purple team skills, validating defensive technology stacks, and helping understand the value of the Assume Breach approach and emulation of threats after getting initial access (C2, post-exploitation, Lateral Movement, Persistence, Evasion).

Contact

- E-mail address: info@defensive-security.com
- Website: https://defensive-security.com
- LinkedIN: https://www.linkedin.com/company/defensive-security/
- Mobile: +48 791 611 309