ABOUT THE COURSE

The Mastering SOC Course stands out from our competitors because its unique features provide students with the knowledge and skills required to succeed in SOC. Mastering Security Operations Centre (SOC) is an advanced combo course covering SOC Analyst and SOC Expert responsibilities to boost your SOC career and enable you to build, run and manage SOC anywhere.

Students learn SOC and SIEM basics, Audit and Log Management in Endpoints, Configuration and Administration of SIEM, EDR and XDR tools, DFIR, adversary simulation, and Real-World Threat Hunting, Phishing.

Instructor-led Online Course

Duration: 30 hours

WHO SHOULD ATTEND ?

- Incident Responders
- Aspiring SOC Analysts
- Threat Researchers
- Information Security Engineers
- Digital Forensic Analysts
- Security Researchers
- SOC Managers
- SOC Analysts

DARKRELAY

Mastering Security Operations Centre (MSOC)

Contact Us.

Visit: www.darkrelay.com
WhatsApp: +91 93805 06281
Email: training@darkrelay.com

COURSE OUTLINE

Lab Setup

- Setting up VirtualBox
- Installing Kali Linux

Fundamentals

- Introduction to Cybersecurity
- Introduction to Linux
- Web Applications 101
- Networking Fundamentals
- Kali Fundamentals
- Windows Fundamentals

Introduction to SOC

- Incident Detection
- Incident Response and Handling
- Responsibilities of SOC Teams
- SOC Deployment Models
- Roles in SOC

Cybersecurity Frameworks for SOC

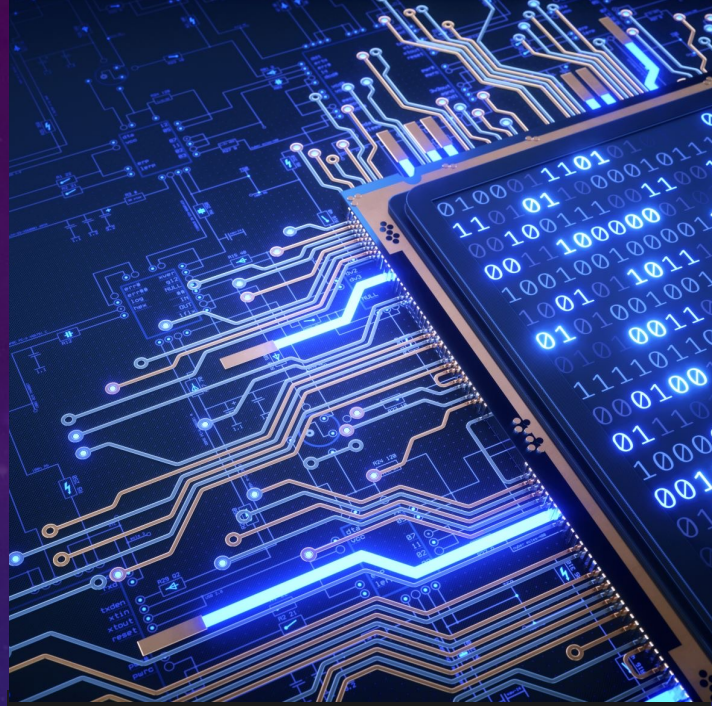
- NIST CSF
- ISO 27001
- CIS Controls
- MITRE ATT&CK

Network Traffic Analysis

- Importance of NTA in SOC
- Wireshark Essentials
- Traffic analysis with Wireshark
- Real World Case Studies

Endpoint Security

- Windows Internals
- Audit Policy
- Sysmon and SysInternals Utilities
- Linux Internals
- Introduction to AntiVirus
- What is an EDR
- Security Hardening



Introduction to SIEM

- Components of SIEM
- Understanding Common Functions
- Using Extension
- Common Event Format
- Syslog
- Linux Event Logs
- Windows Event Logs
- Sysmon Logs

SIEM Practical: Cortex XSIAM

- Architecture
- SIEM
- SOAR
- UEBA
- Play Books
- Query, Visualize, and Monitoring
- Incident Management

Threat Intelligence

- Introduction to TI
- Models for Threat Intelligence
- Threat Intelligence Tools
- Alien Vault
- VulDB
- Virus Total
- Threat Intelligence with Cortex

Adversary Simulation

- Red Team Automation Setup
- Adversary Simulation with RTA

Threat Hunting

- Introduction to Threat Hunting
- IOA
- IOC
- Threat Hunting Methodology
- Threat Hunting with MITRE ATT&CK

XDR

- Introduction to XDR
- XDR vs EDR
- Cortex XDR
- Threat Hunting: Cortex XDR

Digital Forensics

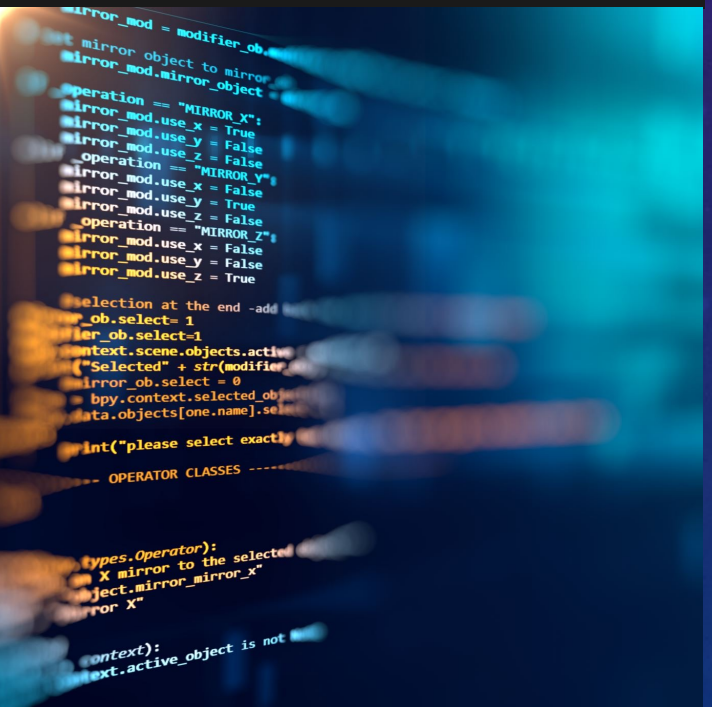
- Introduction
- Autopsy Setup
- Forensics with Autopsy
- Case Studies

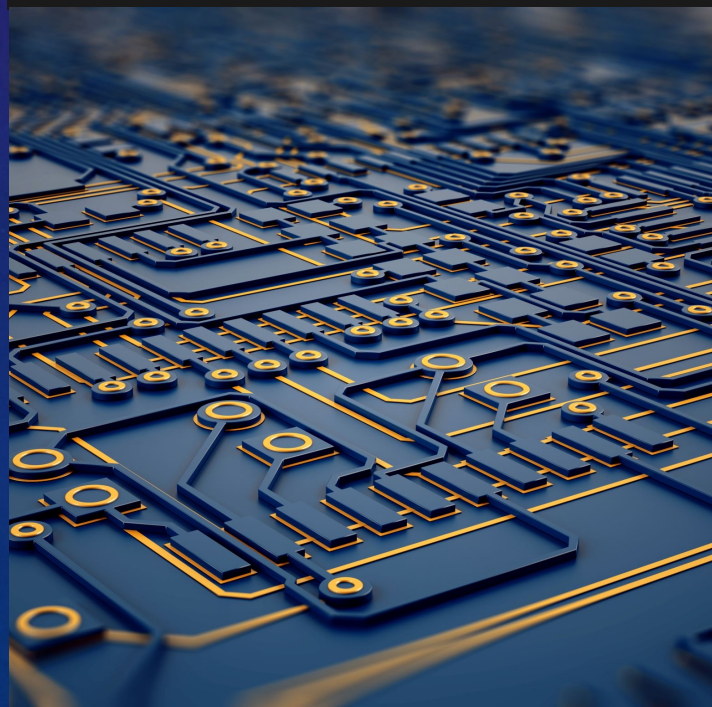
Phishing

- Fundamentals of Phishing
- Analyzing Phishing
- GoPhish Setup
- Phishing with GoPhish

Case Study

- APT3 Adversary Emulation





ABOUT DARKRELAY

Founded in 2019, DarkRelay is lead by Cybersecurity veterans who are SANS 760, GXPN, GPEN, OSCP, OSCE, and CISSP certified with more than 20 years of experience in cyber security research and development.

DarkRelay uses its perspective to build valuable security programs for its students.

Whether you are a beginner or an experienced cyber security professional, our training will address your every learning need, challenge, and career goal.

DARKRELAY

OUR TRAININGS

- Practical Penetration Testing
- Attacking Web Applications
- Fuzzing & Exploit Development
- Red Teaming
- Software Development Security
- Ethical Hacking
- Advanced Penetration Testing
- Vulnerability Assessment
- Malware Analysis
- Cloud Security
- IAM

Mastering Security Operations Centre (MSOC)

For more information

Visit: www.darkrelay.com
WhatsApp: +91 93805 06281
Email: training@darkrelay.com