CADRE 1 // CYBERSECURITY TRAINING PROGRAMME

BlueGuardia

SOC Analyst Bootcamp

14-Week Practitioner Programme · Online · Theory + Hands-On Labs

14	100%	Wazuh
WEEKS	ONLINE	HANDS-ON
Full Programme	Flexible Timing	SIEM · EDR · SOC

// THE OPPORTUNITY

Why Cybersecurity?

The cybersecurity industry is booming. Startups and enterprises worldwide are hiring professionals at scale — and there is still space for new entrants before the market saturates.

> *"One thing more expensive than security is having no security."*
>
> — Industry Proverb

5.5M

Open SOC roles globally

ISC2 2024

+32%

Job growth through 2032

BLS 2024

$112K

Median SOC salary (US)

Glassdoor

67%

Cyber jobs are SOC-related

BLS 2024

ABOUT US

Forging Cyber Defenders

BlueGuardia is a cybersecurity training institute built by practitioners. Our mission: produce job-ready SOC Analysts and Penetration Testers through hands-on, real-world training — then grow into a full Managed Security Service Provider.

// OUR LONG GAME

From training institute to full-service MSSP.

- 24/7 managed SOC services with detection engineering
- Penetration Testing across web, mobile & network
- Vulnerability Assessment & AI Pen Testing
- OT Security Operations & GRC / Compliance

Practitioner-Built

Trainers are active industry professionals, not academics.

Hands-On Labs

Real SIEM, EDR & SOC environments — not slides.

Job-Ready Outcomes

Resume, LinkedIn & interview prep built into the programme.

14 Weeks to SOC Analyst

Weeks 1–4
SECTION 1

Foundation & Theory

- Org context & cybersecurity landscape
- OS & networking fundamentals
- Cybersecurity concepts, CIA Triad, AAA
- Attack types, malware, social engineering

Online · Flexible Scheduling

Weeks 5–12
SECTION 2

All About SOC

- Wazuh & Elastic SIEM setup & investigation
- Phishing Analysis Lab
- MITRE ATT&CK framework (overview)
- OpenEDR · Incident Reporting

Cohort-Based Learning

Weeks 13–14
SECTION 3

Job-Ready Profile

- LinkedIn profile optimisation
- Job-ready resume preparation
- Interview Q&A coaching
- Industry expert sessions

Active SOC Practitioners as Trainers

// SOC ANALYST

Security Operations Center

SOC Analysts are the first responders of the digital world. When alerts fire, they triage, investigate, and contain breaches in real time.

L1 Analyst
Alert triage & initial investigation

L2 Analyst
Deep-dive analysis & escalation

L3 Analyst
Threat hunting & forensics

Skills You Will Build

SIEM Operations

Wazuh & Elastic · log collection · detection rules · use-case creation

Alert Investigation

5 Ws framework · incident response lifecycle · triage methodology

Phishing Analysis

Email header analysis · malicious URL detection · SIEM escalation

MITRE ATT&CK (Overview)

TTPs · mapping alerts to techniques · adversary behaviour

Threat Intelligence

OSINT · IOC enrichment · threat hunting overview

Incident Reporting

Report structure · escalation communication · mock report lab

What You Will Learn

Week 1

Basic Knowledge

- Org structure & cybersecurity roles
- Market trends
- Hardware & Internet basics

Week 2

Cyber Fundamentals

- CIA Triad · AAA · Attack types
- Malware · Phishing · Social Engineering
- Encryption & Hashing

Week 3

Operating Systems

- Windows & Linux basics
- Users · Permissions · Auth
- CLI: CMD & Shell

Week 4

Networking

- TCP/IP · OSI · Subnetting
- Protocols · Firewalls · IDS/IPS
- VPNs · Proxies

Week 5

All About SOC

- L1 / L2 / L3 roles & duties
- SOC tools & environments
- MITRE ATT&CK overview

Weeks 5–12 · LABS

- Wazuh SIEM · Elastic SIEM
- OpenEDR Investigation
- Phishing Analysis Lab
- Incident Reporting
- Threat Hunting Overview

What You Will Work With

SIEM

- Wazuh (primary)
- Elastic / Kibana
- Log ingestion & rules
- Alert investigation

EDR

- OpenEDR
- How EDR works
- EDR vs XDR
- Endpoint telemetry

Investigation

- 5 Ws framework
- Incident Response Lifecycle
- MITRE ATT&CK
- Phishing email analysis

Reporting & TI

- Incident report writing
- Escalation communication
- Threat Intelligence (IOCs)
- OSINT techniques

SOC Awareness

- Active Directory
- Email & Web Gateways
- Exchange Servers
- IAM / PAM overview

Broader Toolset

- SOAR concepts
- WAF & Firewall
- IPS/IDS · NDR
- EPP / Antivirus · FIM

// ADDITIONAL PERKS

More Than Just a Course

Industry Expert Sessions
Live Q&A with senior SOC professionals

Completion Certificate
Recognised credential for your portfolio

LinkedIn Optimisation
Profile review & recruiter-ready guidance

Interview Preparation
Common questions bank + mock sessions

Networking Opportunities
Peer & professional community access

// WHAT YOU WALK OUT WITH

Your Outcomes

- Solid foundation in cybersecurity fundamentals
- Hands-on experience in real SIEM environments
- Practical phishing analysis & incident reporting skills
- Understanding of MITRE ATT&CK & threat intelligence
- Professional LinkedIn profile ready for recruiters
- Interview preparation & common question bank
- Certificate of completion
- Access to a community of practitioners

Train the Talent.

Build the Firm.

Defend the Industry.

Join Cadre 1 and begin your journey into the world of cybersecurity. Limited seats. Real skills. Real outcomes.

Apply Now → blueguardia.com

blueguardia.com