INTERNSETU

Code. Secure. Succeed.

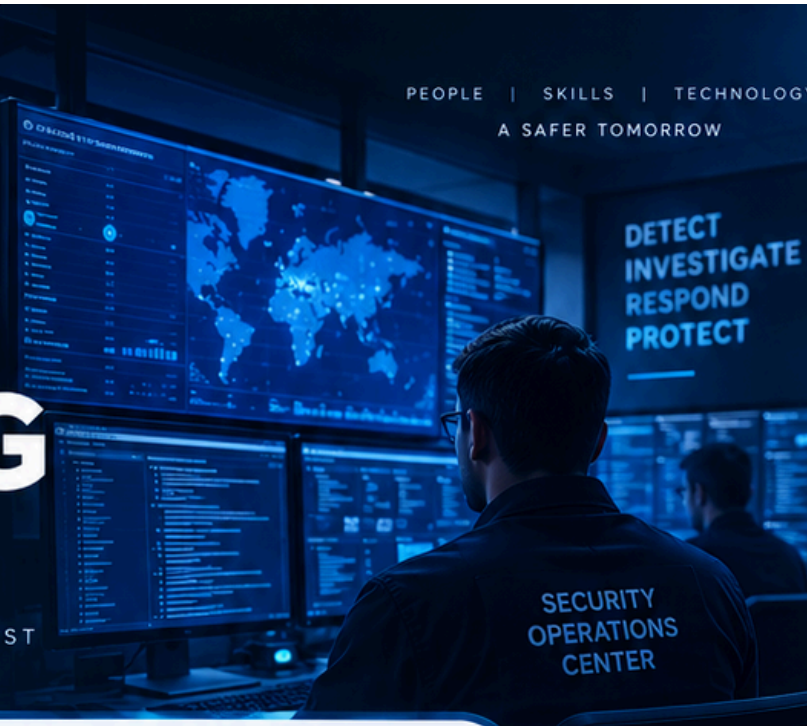
SOC ANALYST

MONITOR | DETECT | RESPOND



INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOG
A SAFER TOMORROW



SOC ANALYST TRAINING

LEARNING PATH

YOUR JOURNEY TO BECOME A SOC ANALYST

MONITOR
ANALYZE
INVESTIGATE
RESPOND
DEFEND

TURNING
KNOWLEDGE
INTO A SAFER
TOMORROW

01 YOU START HERE
Build your foundation and begin your SOC journey

02 SOC FUNDAMENTALS
Understand SOC operations, monitoring and SIEM concepts

03 DIGITAL FORENSICS
Learn to investigate, analyze and uncover evidence

04 INCIDENT RESPONSE
Develop skills to handle and respond to security incidents

05 THREAT INTELLIGENCE
Analyze threats and stay ahead of adversaries

06 SOC ANALYST
Be job-ready with practical skills and real-world experience

"SECURE TODAY
STRONGER
TOMORROW

SKILLS
FOR A
SAFER
DIGITAL WORLD

LEARN | PRACTICE | GROW | SUCCEED

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW

SOC ANALYST TRAINING

COURSE DESCRIPTION

Our SOC Analyst Training program is designed to equip you with the skills and knowledge to monitor, detect, analyze, and respond to cybersecurity threats in real-world environments. Through a hands-on, practical approach, you will learn industry-standard tools, SOC workflows, and incident response techniques to build a strong foundation for a career in cybersecurity.



REAL-WORLD SKILLS
Hands-on labs with industry standard tools and scenarios.

INDUSTRY RELEVANT
Aligned with current SOC operations and security practices.

EXPERT GUIDANCE
Learn from experienced cybersecurity professionals.

CAREER READY
Build the skills and confidence to start your SOC career.

"LEARN TODAY
DEFEND TOMORROW"

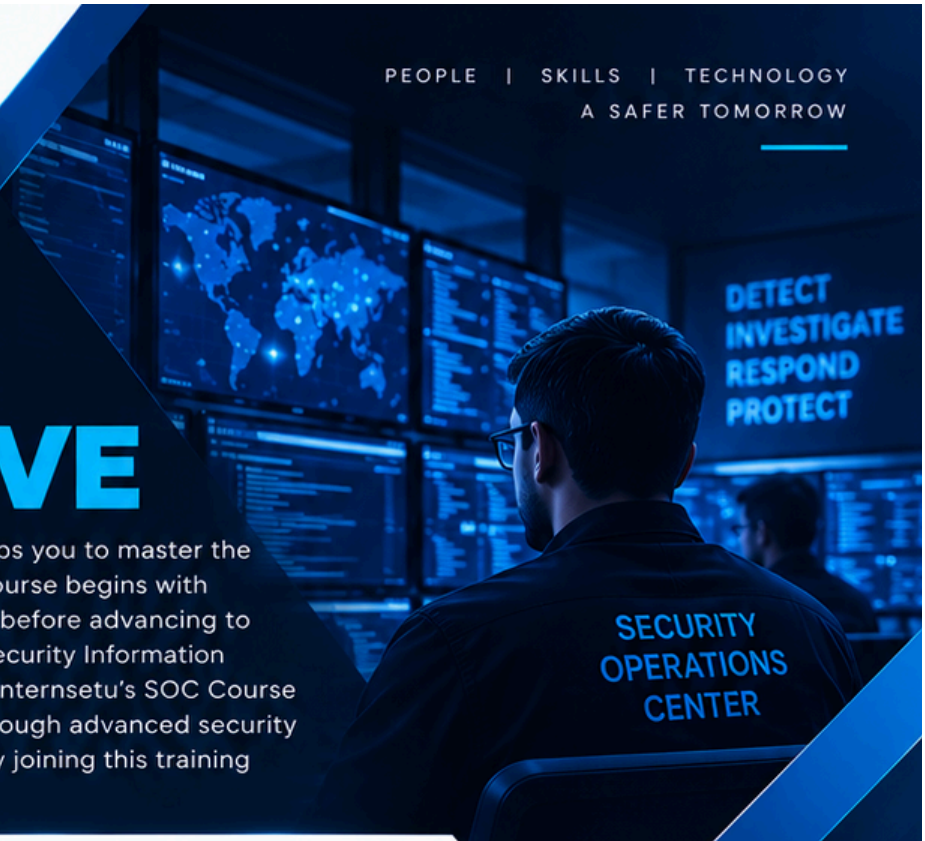
CYBERSECURITY
CAREERS START HERE

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW

SOC ANALYST TRAINING

OUR OBJECTIVE



Our Certified SOC Training Program equips you to master the latest high-demand technical skills. The course begins with intermediate cybersecurity fundamentals before advancing to forensic analysis, threat intelligence, and Security Information and Event Management (SIEM) solutions. Internsetu's SOC Course empowers cybersecurity professionals through advanced security expertise and professional certification. By joining this training program, you will be able to:

01 **IMPLEMENT**
Implement advanced technical strategies, tools, and techniques to safeguard organizational data.

02 **IDENTIFY**
Identify potential threats and develop robust countermeasures to mitigate risks.

03 **MASTER**
Master network forensics and incident response protocols with in-depth analysis.

04 **ACQUIRE**
Acquire comprehensive, cutting-edge cybersecurity industry expertise.

05 **PERFORM**
Perform detailed malware analysis and classification to defend critical assets.

"SKILLED PEOPLE SAFER TOMORROW



DEFEND TODAY
ENABLE A
SAFER TOMORROW

LEARN | PRACTICE | GROW | SUCCEED

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW

SOC ANALYST TRAINING

YOUR PATH TO A STRONGER CYBERSECURITY CAREER



The Certified SOC Analyst credential acts as a powerful launchpad for aspiring security professionals looking to meet the rapidly growing demand across the cybersecurity industry. Earning this certification not only deepens your core understanding of essential SOC operations, but it also empowers you to showcase practical expertise to potential employers, unlock high-growth opportunities across various network security domains, and stay fully up-to-date with the evolving skills needed for L1, L2, and L3 analyst roles—proving your dedicated commitment to mastering complex tasks within a modern security team.

SKILLS TODAY | OPPORTUNITIES TOMORROW

SECURE
MONITOR
RESPOND
TOGETHER

01

EXECUTE

Execute robust technical strategies, tools, and methodologies to protect sensitive organizational data.

02

IDENTIFY

Identify emerging cyber threats and implement effective countermeasures to mitigate security risks.

03

GAIN

Gain deep expertise in network forensics and end-to-end incident response procedures.

04

EXPAND

Expand your fundamental and practical knowledge across the cybersecurity industry landscape.

05

CONDUCT

Conduct thorough analysis and classification of malware to neutralize malicious software.

BUILD SKILLS | UNLOCK OPPORTUNITIES | STAY AHEAD

A SAFER DIGITAL TOMORROW

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW

SOC ANALYST TRAINING

PREREQUISITE

GET READY FOR YOUR SOC JOURNEY



Basic Knowledge

Prior knowledge of Basic Networking knowledge, OS basics, Troubleshooting is recommended.

Relevant Experience

Experience as an entry-level SOC Analyst, Cyber Security Analyst, Information Security role.

Domain Experience

Experience of two years in the Information Security domain.

"A STRONG FOUNDATION LEADS TO GREATER OPPORTUNITIES

TARGET AUDIENCE

THIS PROGRAM IS IDEAL FOR

- Technical Support Engineers
- System Administrator
- Security Consultants
- Cyber Security Analyst
- Security Systems Engineers
- SOC Analysts (Tier I and Tier II)



BUILD YOUR FUTURE IN CYBER SECURITY

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW



"VISIBILITY TODAY. A SAFER TOMORROW

DOMAIN 1

SECURITY OPERATIONS CENTER (SOC)
FUNDAMENTALS & SIEM MASTERY

Build the foundation. Monitor the present. Defend the future.

01 Introduction to SOC & Core Architectures

Building & Functions of a SOC
- Fundamentals of establishing an effective Security Operations Center
- Core operational workflows
- Continuous monitoring strategies

The Heart of SOC – SIEM
- Understanding the central role of Security Information and Event Management (SIEM)
- Evaluating market leaders via Gartner's Magic Quadrant
- Implementing robust SIEM architecture guidelines

Modern SIEM Evolution
- Comparing Managed Detection and Response (MDR) with traditional SIEM deployment models
- Exploring alternative security solutions

02 Deep-Dive SIEM & Monitoring Platforms

ELK Stack & Elastic SIEM
- Platform overview & alert investigations
- Elasticesarch architecture & lifecycle management
- Kibana operations & dashboard creation
- Log ingestion pipeline & custom parsing
- Dynamic alert generation

SecurityOnion
- Architecture & tools overview
- Standalone server deployment
- System operations & diagnostics (sostat)
- Web UI tools & terminal commands
- Traffic simulation using PCAP replay

Splunk Enterprise
- Enterprise requirements & real-world applications
- Cross-industry deployment standards
- Master Search Processing Language (SPL)
- Core terminologies and use cases

AlienVault OSSIM Fundamentals
- Deployment architecture & baseline configuration
- Integrated vulnerability scanning
- Asset discovery and threat detection
- Operational deployment

IBM QRadar SIEM
- Component architecture & event/flow data pathways
- Console navigation
- Offense management
- Health & system monitoring
- Data analysis & threat investigation

Hands-On Toolset Exposure

PRACTICE | ANALYZE | DETECT | DEFEND

ELK Stack | IBM QRadar CE | Splunk | SecurityOnion | AlienVault OSSIM | Wireshark | SGUIL

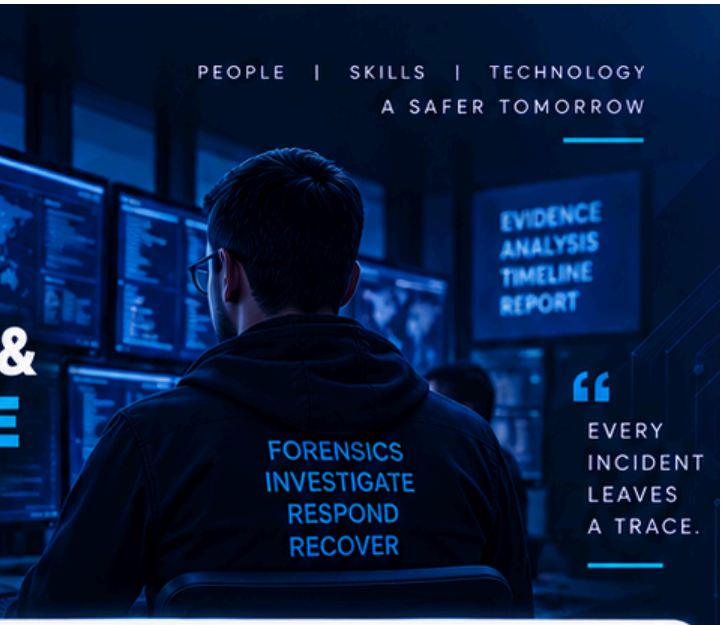


"REAL TOOLS.
REAL SKILLS.
REAL IMPACT.

LEARN | PRACTICE | GROW

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW



DOMAIN 2

DIGITAL FORENSICS & INCIDENT RESPONSE FUNDAMENTALS

Investigate. Analyze. Respond. Preserve the Truth.

"EVERY INCIDENT LEAVES A TRACE."

01 Introduction to Digital Forensics & Incident Response (DFIR)

FOUNDATIONS FOR A SAFER TOMORROW

Core Concepts of Digital Forensics

- Methods and principles for collecting, preserving, and documenting digital evidence associated with cybercrime.

Digital Subject Access Requests (DSAR)

- Handling legal and regulatory obligations for data discovery and personal data extractions.

The Computer Forensics Lifecycle

- Executing the standard forensic methodology—Identification, Preservation, Collection, Examination, Analysis, and Reporting.

Law Enforcement Collaboration

- Defining escalation pathways and distinguishing between internal security incidents and matters requiring law enforcement involvement.

02 Digital Forensics Fundamentals

FROM DATA TO INSIGHTS

Data Representation & File Structures

Data Encoding Formats

- Analyze raw data across Hexadecimal, Octal, and Binary representations.
- Understand structural differences between binary and text files.

Timestamp Formats

- Interpret UNIX Epoch, MAC (Modified, Accessed, Created) times.
- Work with Chrome timestamps and Windows FILETIME values.

Storage Media & File Systems

Magnetic Hard Drive Mechanics

- Explore physical structure (platters, sectors, tracks, clusters).
- Analyze Slack Space for hidden data.

Solid-State Drive (SSD) Forensics

- Understand SSD controller functions.
- Impact of Garbage Collection, TRIM operations, and Wear Leveling algorithms on evidence retention.

File System Forensics

- Architectural fundamentals and key artifacts across FAT16/FAT32, NTFS, EXT3/EXT4, and HFS+/APFS.

Artifact Analysis & Volatility

Metadata Analysis & File Carving

- Extract embedded file attributes.
- Carve raw binary fragments to recover unallocated or deleted data.

Memory & Swap Space Storage

- Examine volatile evidence sources across system RAM.
- Analyze Windows Page File (pagefile.sys) and Hibernation Files (hiberfil.sys).

Order of Volatility

- Prioritize data capture based on life expectancy.
- From CPU registers and RAM to persistent storage media and archived backups.

DIGITAL FORENSICS TURNS DATA INTO ANSWERS.

COLLECT | PRESERVE | ANALYZE | REPORT

INVESTIGATE TODAY FOR A SAFER TOMORROW

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW



"EVIDENCE SPEAKS WHEN OTHERS CAN'T.

DOMAIN 2

DIGITAL FORENSICS & INCIDENT RESPONSE FUNDAMENTALS

Investigate. Analyze. Respond. Preserve the Truth.

03 Forms of Digital Evidence

EVERY TRACE COUNTS

Volatile Evidence Capture

- Gather transient data before system power-down.
- RAM contents, CPU cache, registers, routing tables, ARP caches.
- Active process tables, kernel metrics, temporary file systems, swap space.

Non-Volatile Disk Evidence

- Acquire persistent structures from HDDs and SSDs.
- Analyze file systems, deleted data, and unallocated space.

Network-Based Artifacts

- Collect event logs, active network connections, NetFlow telemetry.
- Packet captures (PCAPs) and proxy logs.

Web & Cloud Evidence

- Extract data from cloud repositories and remote backups.
- Collect direct message logs, forum activity, social media footprints, and online blogs.

Physical Device Targets

- Handle laptops, desktops, mobile devices, external drives.
- Tablets, digital cameras, smartwatches, GPS units and other hardware sources.

04 Chain of Custody & Evidence Handling

PRESERVE TODAY. PROTECT TOMORROW.

Chain of Custody Fundamentals

Understand the legal definition and procedures to maintain continuous, unbroken control of digital evidence.

Integrity & Authenticity

Safeguard evidence admissible in court by establishing strict examiner authenticity and verifiable data integrity.

Standard Operational Guidelines

Follow industry best practices for secure evidence handling and analysis.

Evidence Logging & Documentation

- Maintain meticulous transfer, storage, and handling records.

Cryptographic Hashing

- Generate baseline hash values (MD5, SHA-256) at acquisition to verify zero tamper/modification over time.

Hardware & Software Write-Blockers

- Prevent media modification during the imaging process.

Forensic Duplicate Processing

- Ensure all analysis is conducted on forensically sound copies rather than original evidence.

05 Windows Forensic Investigations

UNCOVER. ANALYZE. CONNECT THE DOTS.

Windows Registry

- Extract system configuration, user activity, MRU lists, and connected USB histories.

Event Logs

- Analyze Security, System, Application, and PowerShell logs for intrusion indicators.

Execution Artifacts

- Examine Prefetch files, .LNK shortcuts, system DLLs, and Jump Lists to prove program execution.

Persistence Mechanisms

- Investigate services, drivers, autorun files, malicious directories (AppData, Temp), and Scheduled Tasks.

Forensic Limitations & Case Scenarios

- Recognize anti-forensic techniques, log wiping, encryption barriers.
- Walk through real-world scenarios: compromise analysis, insider threats, and malware persistence hunts.

"FORENSICS REVEALS THE TRUTH. DISCIPLINE KEEPS IT INTACT.

COLLECT › ANALYZE › REPORT › RESPOND

SAME EVIDENCE. A SAFER TOMORROW.

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW



DOMAIN 2

DIGITAL FORENSICS & INCIDENT RESPONSE FUNDAMENTALS

Investigate. Analyze. Respond. Reeserve the Truth.

06 Linux/Unix (*nix) Investigations & Artifact Collection

DIFFERENT SYSTEMS. SAME TRUTH.

*nix Forensic Artifacts

- Analyze system logs (/var/log), .bash_history, active processes (/proc), cron jobs, SSH authorized keys, system services, and persistent daemon configurations.

Limitations

- Custom kernel configurations
- Rootkits
- Log manipulation
- Diverse file system types (Ext4, XFS, ZFS)

Investigation Scenarios

- Analyze Linux server compromises
- Investigate unauthorized access attempts
- Identify privilege escalations

Evidence Collection Prerequisites & Hardware

Physical Equipment

- Anti-static bags, Faraday bags
- Evidence tags, sterile drives
- Forensic workstations
- Hardware disk imagers
- Write-blockers, interface cables
- Blank media, cameras

Forensic Software Tools

- Wireshark, NetworkMiner and related traffic parsers

Legal Standards (ACPO Principles)

- Follow Good Practice Guides for Computer-Based Electronic Evidence to ensure court admissibility.

07 Live Forensics & Real-Time Acquisition

CAPTURE TODAY. PREVENT TOMORROW.

Live Acquisition Fundamentals

- Execute live volatile data extraction on running systems.
- Capture unencrypted data, running processes, and active network connections without initiating system shutdown.
- Fast-path collection of critical system artifacts and configuration files.

Enterprise Analysis Tools

- Utilize agent-based systems and enterprise solution suites (Carbon Black, EnCase).
- Leverage live memory collectors and custom automation scripts.
- Collect tactical evidence from laptops, desktops, mobile devices, websites, forums, blogs, social media profiles, and chat logs.

Risk & Impact Management

- Assess potential evidence contamination or system instability caused by running live acquisition scripts.
- Balance data collection needs with operational impact.
- Follow proven methodologies to minimize risk on compromised hosts.

08 Post-Investigation Standards

DOCUMENT. PRESERVE. CLOSE SECURELY.

Forensic Report Writing

- Structure clear, objective technical reports.
- Tailor reports for legal teams, executives, and technical audiences.
- Include findings, methodologies, and evidentiary details.

Evidence Retention Mandates

- Manage storage lifecycles in compliance with legal retention periods.
- Adhere to organizational and regulatory requirements.
- Maintain evidentiary integrity over time.

Secure Evidence Destruction

- Implement compliant, irreversible media sanitation methods.
- Use physical shredding, cryptographic wiping, multi-pass overwriting, and magnetic degaussing.
- Ensure proper documentation of destruction processes.

Hands-On DFIR Toolset Exposure

REAL TOOLS. REAL INVESTIGATIONS. REAL SKILLS.

Windows & Linux CLI	FTK Imager	Magnet RAM Capture	Autopsy Forensic Browser	Volatility & Volatility Workbench	EnCase Forensic

INTERNSETU
Code. Secure. Succeed.

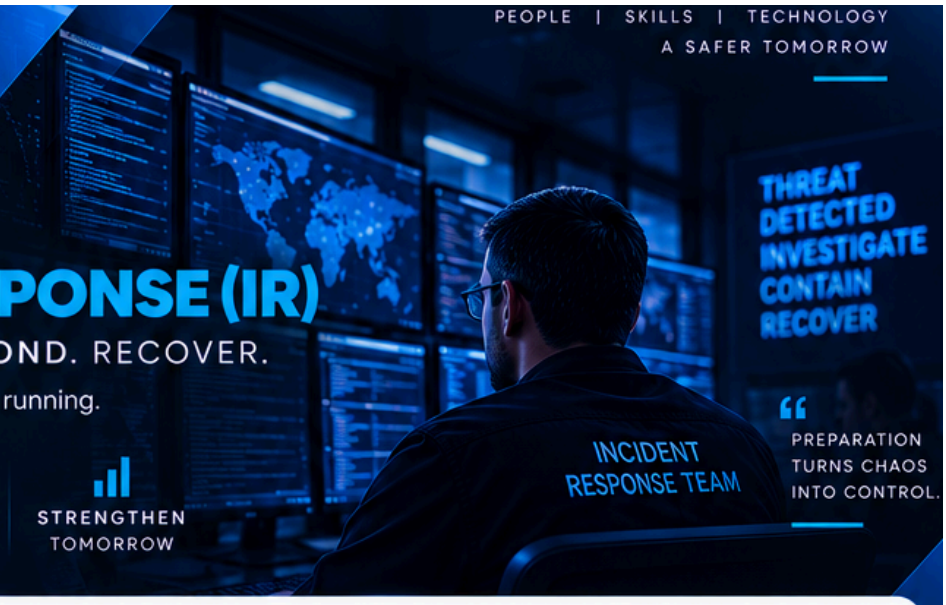
PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW

DOMAIN 3

INCIDENT RESPONSE (IR)

DETECT. CONTAIN. RESPOND. RECOVER.

Be ready. Be resilient. Keep business running.



PREPARE TODAY | RESPOND EFFECTIVELY | MINIMIZE IMPACT | STRENGTHEN TOMORROW

01 Introduction to Incident Response

FROM EVENTS TO RESILIENCE

Core Concepts

- Defining Incident Response and its role in protecting operational continuity and organizational assets.

Events vs. Incidents

- Distinguishing between benign system events and verified security incidents that compromise confidentiality, integrity, or availability.

Frameworks & Methodologies

NIST SP 800-61 Rev. 2 Lifecycle

- Standardized operational phases: Preparation; Detection & Analysis; Containment, Eradication & Recovery; and Post-Incident Activity.

Lockheed Martin Cyber Kill Chain

- Tracking adversary operational stages (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Actions on Objectives) to disrupt attacks early.

MITRE ATT&CK Framework

- Utilizing a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) to map threats and validate security coverage.

02 IR Preparation Phase

PLAN. BUILD. DEFEND.

Planning, Strategy & Asset Identification

Governance Foundations

- Develop comprehensive Incident Response Plans, Policies, and operational Playbooks/Procedures.

CSIRT Structure

- Define roles, responsibilities, and communication paths for the Computer Security Incident Response Team (CSIRT).

Asset Discovery & Risk Assessment

- Categorize critical infrastructure, software inventory, and identify High-Value Assets (HVAs).

Decoy Infrastructure

- Design Demilitarized Zones (DMZs) and deploy honeypots/ deceptive elements to detect unauthorized lateral movement.

Multi-Layered Defense Systems

Host-Based Defenses

- Endpoint Detection & Response (EDR) and Antivirus (AV) deployments.
- Host Intrusion/Dotection Systems (HIDS).
- Local host firewalls, account access control, and Group Policy Objects (GPO) hardening.

Network Defenses

- Network Intrusion Detection & Prevention Systems (NIDS/NIPS).
- Edge firewalls, web proxy servers.
- Network Access Control (NAC) enforcement.

Email Defenses

- Inbound spam filtering.
- Attachment filtering.
- Dynamic attachment sandboxing.
- External email tagging.

Physical Defenses

- Physical deterrents.
- Facility access controls.
- Environmental/ surveillance monitoring controls.

Human-Centric Defenses

- Continuous security awareness training.
- Policy enforcement.
- Security-positive incentive programs.

A WELL-PREPARED ORGANIZATION RESPONDS FASTER AND RECOVERS STRONGER.

PEOPLE | PROCESSES | TECHNOLOGY

PREPARE TODAY FOR A SAFER TOMORROW.

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW

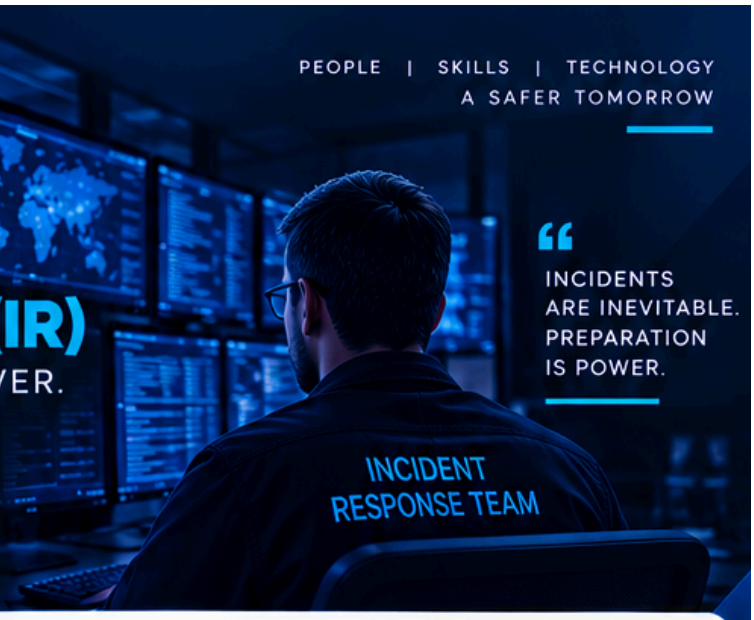
DOMAIN 3

INCIDENT RESPONSE (IR)

DETECT. CONTAIN. RESPOND. RECOVER.

Be ready. Be resilient. Keep business running.

PREPARE TODAY | DETECT FASTER | RESPOND SMARTER | RECOVER STRONGER



"INCIDENTS ARE INEVITABLE. PREPARATION IS POWER."

03 Detection & Analysis Phase

ANALYZE. INVESTIGATE. ISOLATE.

Common Security Incidents

- Malware infections
- Unauthorized access attempts
- Data exfiltration
- Denial-of-service (DoS) attacks
- Insider threats

Baseline Profiling

- Establish operational baselines.
- User/entity behavior analytics (UEBA).
- Detect abnormal network, user, or system activities.

Centralized Logging & Aggregation

- Ingest and normalize multi-source logs.
- Unified visibility across endpoints, firewalls, and applications.

Threat Correlation & Analysis

- Apply SIEM correlation rules.
- Use threat intelligence feeds.
- Cross-event linking.
- Isolate true positives.
- Prioritize severity.

04 Containment, Eradication & Recovery Phase

CONTAIN. ELIMINATE. RESTORE.

CSIRT & CERT Operational Roles

- Define structure & responsibilities.
- Understand differences between CSIRT and CERT.

Targeted Containment Strategies

- Isolate hosts / networks.
- Dynamic VLAN segregation.
- Selective shutdown.
- Divert to honeypots / deception lures.

Forensic Evidence Preservation

- Secure volatile RAM and disk images.
- Maintain legal & operational evidence chains.

Eradication & Artefact Removal

- Locate and remove malicious binaries, web shells, backdoors.
- Eliminate persistence mechanisms.

Root Cause Analysis & System Recovery

- Identify initial attack vector.
- Apply patches.
- Harden configurations.
- Restore from clean backups.
- Return to trusted production.

05 Lessons Learned Phase

IMPROVE. COMPLY. STRENGTHEN.

Incident Review & Debriefing

- Evaluate response timeline effectiveness.
- Capture operational highlights.
- Identify communication gaps.
- Address procedural bottlenecks.

Documentation & Playbook Refinement

- Update incident response runbooks.
- Maintain clear audit trails for compliance.

Metrics & Executive Reporting

- Track KPIs (MTTD & MTTR).
- Quantify security posture improvements for leadership.

Hands-On Incident Response Toolset Exposure

REAL TOOLS. REAL INVESTIGATIONS. REAL IMPACT.

Sysinternals Suite (Process Explorer, Autoruns, ProcMon)	Hash Calculator	Threat Intelligence & Online Search Engines (VirusTotal, AbuseIPDB, Any.Run)	CyberChef	Wireshark	NetworkMiner

INTERNSETU
Code. Secure. Succeed.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW



COLLECT
ANALYZE
CONNECT
ANTICIPATE
STAY AHEAD

DOMAIN 4

THREAT INTELLIGENCE (CTI)

FROM INSIGHTS TO ACTION.

Understand threats. Enrich defenses. Stay ahead.

OBSERVE THE THREAT | UNDERSTAND THE ADVERSARY | ENRICH SECURITY | STAY PROACTIVE

"KNOW THE THRE OUTPACE THE ATTA

01 Introduction to Cyber Threat Intelligence

TURNING INFORMATION INTO A SAFER TOMORROW

Threat Intelligence Concepts

- Define CTI and its role in transforming raw data into actionable security insights to anticipate, prevent, and respond to cyber threats.

Strategic Value of CTI

- Enhance situational awareness.
- Accelerate incident investigations.
- Enrich SIEM/EDR alerts.
- Proactively reduce the enterprise attack surface.

Limitations & Challenges

- Attribution complexity.
- Reactive nature of static indicators.
- Stale Indicators of Compromise (IOCs).
- False positives.

Emerging Trends in CTI

- Dynamic risk scoring systems (e.g., Predictive Prioritization).
- Blend real-time threat intelligence with vulnerability management data.
- Stay ahead with AI and automation.

Traditional Intelligence Disciplines

- OSINT – Open Source Intelligence
- SIGINT – Signals Intelligence
- HUMINT – Human Intelligence
- GEOINT – Geospatial Intelligence

02 Threat Actors & Adversary Profiling

KNOW WHO. WHY. HOW. AND WHAT THEY TARGET.

Threat Actor Taxonomy

- Cybercriminals
- Hacktivists
- Malicious insider threats
- Nation-State Advanced Persistent Threats (APTs)

Adversary Motivations

- Financial gain
- Political agendas
- Espionage
- Ideology
- Competitive advantage

Technical Capability & Skill Spectrum

- Script kiddies
- Opportunistic hackers
- Skilled and well-resourced criminal groups
- Highly organized APT groups

Adversary Naming Conventions

- CrowdStrike's animal themes (e.g., Bear, Falcon)
- Mandiant's APT numbering (e.g., APT28)
- Microsoft's weather-based taxonomy (e.g., Storm series)
- Understand cross-vendor naming variations

Targeting Patterns

- High-risk industry verticals (e.g., Finance, Healthcare, Energy)
- Critical national infrastructure
- Government entities
- Specific corporate profiles targeted by specialized adversary groups

INTELLIGENCE-DRIVEN DEFENSE LIFECYCLE

COLLECT INTELLIGENCE → ANALYZE AND ENRICH → CORRELATE AND CONTEXTUALIZE → APPLY IN DEFENSE → STAY AHEAD OF EMERGING THREATS

THREAT INTELLIGENCE FUELS A STRONGER MORE RESILIENT TOMORROW.

INTERNSETU
Code. Secure. Succeed.

INTELLIGENCE TODAY. SAFER TOMORROW.

PEOPLE | SKILLS | TECHNOLOGY
A SAFER TOMORROW

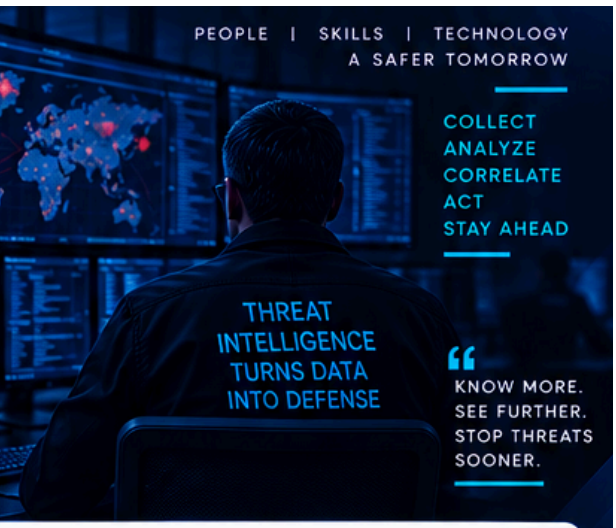
COLLECT
ANALYZE
CORRELATE
ACT
STAY AHEAD

DOMAIN 4

THREAT INTELLIGENCE (CTI)

OPERATIONAL | TACTICAL | STRATEGIC

Turn information into intelligence. Turn intelligence into action.



"KNOW MORE. SEE FURTHER. STOP THREATS SOONER.

OBSERVE THREATS | ANALYZE CONTEXT | SHARE INTELLIGENCE | STRENGTHEN DEFENSES

04 Tactical Threat Intelligence

ACTIONABLE INTELLIGENCE. REAL-WORLD IMPACT.

Threat Exposure Checks (TECs)
- Audit internal environments for current or historical IOCs.

Watchlists & IOC Monitoring
- Deploy IOC feeds across SIEM, IDPS, AV, EDR and firewalls.

Public Exposure Assessments (PEAs)
- Use Google Dorks, theHarvester and social media profiling to find exposed assets.

Open-Web Intelligence Collection
- Automate OSINT collection for threat trends, IP reputation and domain registrations.

Dark-Web Intelligence Collection
- Monitor underground forums, TOR networks and breach repositories for credentials, malware and threat actor activity.

MISP Platform
- Setup and deploy MISP for storing, correlating and sharing structured threat data.

Intelligence Sharing Networks
- Collaborate with CERTs, US-CERT, NCSC and industry ISACs.

IOC/TTP Gathering & Distribution
- Automate ingestion and sharing using STIX/TAXII.

Campaign Tracking & Situational Awareness
- Track active threat campaigns to inform defense postures.

Platform Feasibility & Proof-of-Value (PoV)
- Evaluate and test emerging CTI platforms before enterprise deployment.

OSINT vs. Paid-For Threat Feeds
- Compare open-source feeds with commercial Threat intelligence Vendors (TIVs).

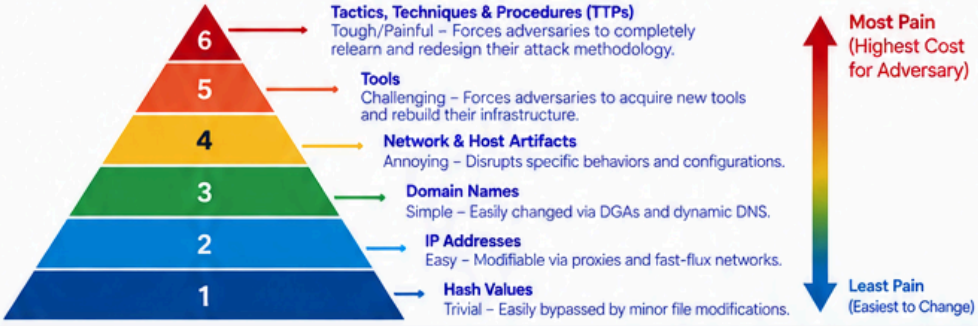
05 David Bianco's Pyramid of Pain

THE HIGHER THE PAIN, THE HARDER THEY FALL.

Concept & Operational Impact

Blocking different indicator types inflicts varying degrees of friction ("pain") on adversaries, increasing their operational cost.

> *"Move up the pyramid, make it harder for the adversary."*



06 Strategic Threat Intelligence

ANTICIPATE. UNDERSTAND. OUTPACE.

IOCs vs. Precursors
- IOCs: Evidence of compromise (e.g., hashes, C2 IPs).
- Precursors: Early warning signs (e.g., scans, domain spoofing, leak chatter).

Tactics, Techniques and Procedures (TTPs)
- Analyze adversary behavior to build proactive, behavior-based defenses.

Adversary Framework Mapping
- MITRE ATT&CK Framework
- Lockheed Martin Cyber Kill Chain

Attribution Challenges & Limitations
- False-flag operations
- Shared infrastructure
- Proxy networks
- Copycat threat groups

07 Malware Analysis & Global Threat Campaigns

LEARN FROM THE PAST. STOP THE NEXT.

Malware Taxonomy & Characteristics
- Trojans
- Ransomware
- Logic Bombs
- Remote Access Trojans (RATs)
- Backdoors

Globally Recognized Threat Campaigns
- Emotet
- Magecart (Web-skimming)
- IcedID
- Sodinokibi (REvil)
- TrickBot
- LokiBot

Hands-On Threat Intelligence Toolset Exposure

REAL TOOLS. REAL INTELLIGENCE. REAL SKILLS.

- **AlienVault OTX** (Open Threat Exchange)
- **MITRE ATT&CK Navigator & Matrices**
- **MISP Platform**
- **Maltego** (Link Analysis & Visual OSINT)
- **VirusTotal**
- **Shodan**
- **Censys**
- **AbuseIPDB**

Online Intelligence Feeds & Repositories

