Table Of Contents

Dozens of Scenarios, Endless Possibilities .......................................................... 3

Incident Response Courses ................................................................................... 4

  Incident Response 101 ....................................................................................... 5
  Enterprise Incident Response .......................................................................... 6

Cyber Security Certification Courses ................................................................. 7

  Cyber Security Forensics Analyst ................................................................. 8
  SOC Analyst Onboarding ............................................................................... 9

Skill Workshops .................................................................................................... 10

  Advanced Malware Forensics ........................................................... 11
  Intrusion Detection ....................................................................................... 12
  SCADA Security ............................................................................................ 13

Conclusion ........................................................................................................... 14

Range customers speak out .............................................................................. 15
Dozens of Scenarios, Endless Possibilities

Cyberbit Range is the world leading cyber simulation and training platform, providing the ability to emulate any type of network and simulate any cyber security scenario to train and test people, procedures and technologies.

Cyberbit Range was built by security experts to prepare analysts for real-life attacks, offering dozens of hyper-realistic cyber security scenarios. Each scenario teaches a set of incident response and cyber security skills, providing analysts with relevant tools and methodologies to operate a cyber-attack across a variety of attack scenarios, platforms and technologies. The scenarios can be run over the course of a couple hours, to a full day, giving all skill levels the chance to hone their analysis and incident response skills. Different combinations of these scenarios can be used to build many types of cyber security courses, as the scenarios vary in difficulty level, attack vectors, technologies used, and skill focus.

In this whitepaper, we will describe a few of the many cyber security courses and workshops that can be built by combining theoretical learning and hyper-realistic simulation training using the Cyberbit Range platform.
Incident response teams and SOC analysts need to constantly refresh their knowledge and skills to remain updated with the everlasting changes in the cyber security threat landscape. Delivering hyper-realistic cyber training scenarios updated with the most relevant and current threats improves incident handling, teamwork, compliance skills, workflows, runbook usage, and other operational skills which are crucial to the success of the incident response operation.
Incident Response 101

**Audience:** Novice SOC Analysts

**Prerequisites:** Basic SOC Experience and Cyber Knowledge

**Duration:** 2 weeks – consecutive, or split in to five 3-day sessions

**Skills Acquired:**
- Deepen familiarity with enterprise runbooks and workflows
- Recognize common threat behaviors and attack vectors
- Use incident response best practices when handling threat alerts
- Perform forensics data collection and investigations after an attack

**Range Scenarios:** SQL Injection, DDOS SYN Flood, Trojan Data Leakage, Trojan Share Privilege Escalation

These scenarios qualify analysts in responding to frequently encountered cyber-attacks. The scenarios aim to challenge the trainees and give them practice and success in many attack vectors. This course focuses on incident response performance while using common SOC procedures and understanding the critical processes in the organization.

**Example Schedule:**

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Networking and</td>
<td>Vulnerabilities, Malware</td>
<td>Incident Response</td>
<td>Range Scenario: SQL Injection</td>
<td>Anatomy of a Cyber-Attack</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>and Hacking</td>
<td>Processes and Technologies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Week 2 | Range Scenario:         | Investigation and              | Range Scenario:                 | Range Scenario: Trojan Share      | Course Summary                             |
|--------| DDOS SYN Flood          | Forensics                      | Trojan Data Leakage              | Privilege Escalation               |                                            |

---

[Image]
Enterprise Incident Response

**Audience:** Active SOC Teams

**Prerequisites:** Networking and Cyber Security Knowledge, SOC Experience

**Duration:** 1 week – consecutive, or five 1-day sessions spread over 5 months

**Skills Acquired:**
- Become updated on the newest cyber threats
- Enhance existing SOC procedures and workflows
- Improve cross-organizational collaboration
- Hunt threats across the enterprise network

**Range Scenarios:** SQL Injection, DDOS SYN Flood, Trojan Data Leakage, Trojan Share Privilege Escalation

The goal of this fast-pace course is to bring SOC teams up-to-date with the current cyber-threat landscape, including both knowledge and hands-on incident response, as well as to streamline their existing workflows and processes. The scenarios used in this workshop are Advanced level scenarios, giving the analysts a chance to deal with complex cyber-attacks alongside their team members while practicing teamwork, escalation processes and advanced cyber security practices.

**Example Schedule:**

<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New Threats Review</td>
<td>SOC Workflows and Playbooks</td>
<td>Teamwork in the SOC and Escalation Procedures</td>
<td>Cross-Organizational Collaboration</td>
<td>Enterprise Incident Response and Threat Hunting</td>
</tr>
<tr>
<td></td>
<td>Range Scenario: Ransomware</td>
<td>Range Scenario: Java SendMail</td>
<td>Range Scenario: DB Dump via FTP Exploit</td>
<td>Range Scenario: WPAD Man-in-the-Middle</td>
<td>Range Scenario: Windows Management Instrumentation Worm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cyber Security Certification Courses

Cyber Security personnel who want to set themselves apart in the job market look for certifications in their domain of choice. Whether they are completely new to the industry, or are looking to improve their resume, these personnel are on the constant lookout for the best certification. Cyberbit Range enables to build certification training courses and tests using the various scenarios, which range in difficulty and skills acquired.
Cyber Security Forensics Analyst

**Audience:** First-Time Analysts

**Prerequisites:** None

**Duration:** 6 weeks

**Skills Acquired:**
- Define and use cyber security concepts and terminology
- Understand network architecture and infrastructure
- Recognize malware and hacking behaviors
- Collect forensics data and investigate a cyber-attack

**Range Scenarios:** SQL Injection, Killer Trojan, DDOS SYN Flood, Apache Shutdown, Java NMS Kill, Java SendMail, Trojan Data Leakage, DB Dump via FTP Exploit, Trojan Share Privilege Escalation, Windows Management Instrumentation Worm

This gives inexperienced trainees the skills to perform quality attack forensics. The course teaches a technological base, followed by an analysis of different aspects of cyber security. The scenarios in the cyber Security Forensics course combine incident response and analysis with extensive forensics on a multitude of technologies and platforms. The trainees will learn to understand adversary motives, and will practice investigation of realistic, complex attacks. The scenarios vary in functionality and motives, from DDOS attacks to espionage, giving new analysts an understanding of the different attacks and threats.

The course includes two tests. Trainees must pass both to receive certification.

---

### Example Schedule:

<table>
<thead>
<tr>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1 Networking and Communications</td>
<td>Networking and Communications</td>
<td>Operating Systems</td>
<td>Network Security and Authentication</td>
<td>Network Security and Authentication</td>
</tr>
<tr>
<td>Week 2 Cyber Terminology and Basics</td>
<td>Vulnerabilities, aware and Hacking</td>
<td>Vulnerabilities, aware and Hacking</td>
<td>The Cyber Kill Chain - Explanation and demonstration on major attacks in history</td>
<td>Anatomy of a Cyber-Attack: Explanation and demonstration on major attacks in history</td>
</tr>
<tr>
<td>Week 3 Data, Databases and Logging + Forensics Tools</td>
<td>Infection Forensics: How to think like an adversary</td>
<td>Range Simulation: SQL Injection</td>
<td>Machine Forensics</td>
<td>Range Simulation: Killer Trojan</td>
</tr>
<tr>
<td>Week 4 Network Forensics</td>
<td>Range Simulation: DDOS SYN Flood</td>
<td>Linux</td>
<td>Linux Forensics</td>
<td>Practice Scenario: Apache Shutdown</td>
</tr>
<tr>
<td>Week 5 Range Simulation: Java NMS Kill</td>
<td>Test Preparation 1: Java SendMail</td>
<td>Espionage and Data Breaches</td>
<td>Range Scenario: Trojan Data Leakage</td>
<td>Test Preparation 2: DB Dump via FTP Exploit</td>
</tr>
<tr>
<td>Week 6 Infection Prevention and Remediation</td>
<td>Review Day + Study Time</td>
<td>Certification Test Part 1: Trojan Share Privilege Escalation</td>
<td>Certification Test Part 2: Windows Management Instrumentation Worm</td>
<td>Course Summary</td>
</tr>
</tbody>
</table>
SOC Analyst Onboarding

**Audience:** Novice Analysts and IT Personnel

**Prerequisites:** Basic Cyber Security Knowledge

**Duration:** 4 weeks

**Skills Acquired:**
- Understand the build and operations of a modern SOC
- Know how to use SOC technologies and management systems
- Become familiar with cyber-attack types and adversary motivations
- Use incident response best practices when handling threat alerts

**Range Scenarios:** SQL Injection, Apache Shutdown, Killer Trojan, Trojan Data Leakage, DB Dump via FTP Exploit, DDOS DNS Amplification, Java SendMail, Ransomware, WPAD Man-in-the-Middle

This course prepares personnel looking to enter SOC Analyst positions in operating real-life cyber-attacks, and can be used by organizations to train new hires. The course focuses on the different aspects of security operations – from how the SOC is built, the tools and processes involved in incident response, and teamwork in the SOC, to an understanding of the different threats that a SOC analyst can encounter during a shift. The scenarios included in this course focus on the SOC analyst’s most important skills, including fast incident response, data loss protection, and attack forensics.

The course includes two tests. Trainees must pass both to receive certification.

**Example Schedule:**

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction to Security Operations</td>
<td>SOC Daily Life and Main Technologies</td>
<td>Teamwork and Operations in the SOC</td>
<td>Incident Response Processes</td>
<td>Range Scenario: SQL Injection</td>
</tr>
<tr>
<td>Week 2</td>
<td>Vulnerabilities, Malware and Hacking</td>
<td>Adversary Motivations and APTs</td>
<td>Kill Chain Analysis</td>
<td>Range Scenario: Apache Shutdown</td>
<td>Range Scenario: Killer Trojan</td>
</tr>
<tr>
<td>Week 3</td>
<td>Data Loss Protection</td>
<td>Range Scenario: Trojan Data Leakage</td>
<td>Range Scenario: DB Dump via FTP Exploit</td>
<td>Forensics and Investigation</td>
<td>Range Scenario: DDOS DNS Amplification</td>
</tr>
<tr>
<td>Week 4</td>
<td>Test Preparation: Java SendMail</td>
<td>Cryptography and Ransomware</td>
<td>Certification Test Part 1: Ransomware</td>
<td>Certification Test Part 2: WPAD Man-in-the-Middle</td>
<td>Course Summary</td>
</tr>
</tbody>
</table>
Skill Workshops

Whether looking to learn a new skill, or to improve an existing one, cyber security personnel (and their employers) strive to constantly stay updated and one step ahead of competitors. Skill workshops are short and focused, providing the opportunity to improve specific skills, and learn new ones, without losing more than a couple days of work time.
Advanced Malware Forensics

**Audience:** Tier 2 Analysts

**Prerequisites:** Cyber Security Knowledge and Experience

**Duration:** 3 Days - consecutive, or spread throughout the year

**Skills Acquired:**
- Enhance understanding of how a cyber-attack works
- Understand which evidence should be collected post-mortem and how
- Sharpen Linux forensics techniques and logging research
- Improve networking and memory forensics capabilities

**Range Scenarios:** Windows Management Instrumentation Worm, Java SendMail, Ransomware

Each scenario in this course is tailored to improving the analysts’ performance in a forensics practice, while training them on responding to a full-scale attack in a realistic scenario. During the course, analysts will “think like the adversaries” and perform professional analysis and response during a simulated attack. The analysts will learn what to look for, where to look, and how to obtain the information that they need.

**Example Schedule:**

<table>
<thead>
<tr>
<th></th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Morning</strong></td>
<td>Advanced Network Forensics</td>
<td>Linux Forensics</td>
<td>Memory Forensics</td>
</tr>
<tr>
<td><strong>Afternoon</strong></td>
<td>Range Scenario: Windows Management Instrumentation Worm</td>
<td>Range Scenario: Java SendMail</td>
<td>Range Scenario: Ransomware</td>
</tr>
</tbody>
</table>

[Image -0x621 to 595x843]
# Intrusion Detection

**Audience:** Tier 1 Analysts  
**Prerequisites:** Basic Networking and Cyber Security Knowledge  
**Duration:** 3 Days - consecutive, or dispersed throughout the year  

**Skills Acquired:**  
- Familiarity with common protocols and malicious protocol abuse  
- Ability to analyze logs and network traffic to uncover intrusions and malware  
- Use network forensics tools and best practices to investigate an intrusion  

**Range Scenarios:** DDoS SYN Flood, SQL Injection, Killer Trojan  

This course is aimed at training beginner Tier 1 SOC analysts at performing intrusion detection analysis by investigating network traffic. The scenarios in this course are built to train analysts in logging research, packet analysis and network forensics.

**Example Schedule:**

<table>
<thead>
<tr>
<th></th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Morning</strong></td>
<td>Traffic and Protocol Analysis</td>
<td>Network Forensics Part 1</td>
<td>Network Forensics Part 2</td>
</tr>
<tr>
<td><strong>Afternoon</strong></td>
<td>Range Scenario: DDoS SYN Flood</td>
<td>Range Scenario: SQL Injection</td>
<td>Range Scenario: Killer Trojan</td>
</tr>
</tbody>
</table>
SCADA Security

**Audience:** Tier 1 and Tier 2 Analysts

**Prerequisites:** Cyber Security Knowledge

**Duration:** 5 Days – consecutive

**Skills Acquired:**
- Understand the unique challenges in protecting Critical Infrastructures
- Familiarity with SCADA protocols and how to analyze them
- Ability to investigate an attack across both IT and OT systems
- Use proper response tactics to an IT/OT attack

**Range Scenarios:** SCADA HMI, SCADA VPN, SCADA Field to Field

This course gives analysts a deep understanding of Critical Infrastructures and SCADA networks, as well as the tools to provide incident response during a SCADA attack.

**Example Schedule:**

<table>
<thead>
<tr>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morning</td>
<td>Day 2</td>
<td>Day 3</td>
<td>Day 4</td>
<td>Day 5</td>
</tr>
<tr>
<td>The IT/OT/IOT Challenge</td>
<td>Understanding SCADA Protocols Part 1</td>
<td>SCADA Malware and Attack History</td>
<td>SCADA Intrusion Detection</td>
<td>Advanced SCADA Forensics</td>
</tr>
<tr>
<td>SCADA Network Infrastructures</td>
<td>Understanding SCADA Protocols Part 2</td>
<td>Range Scenario: SCADA HMI</td>
<td>Range Scenario: SCADA VPN</td>
<td>Range Scenario: SCADA Field to Field</td>
</tr>
</tbody>
</table>

---

[Image -0x621 to 595x843]
Conclusion

In the face of endless cyber threats, performing the best protection, detection and response to a cyber-attack requires a well-trained workforce. Preparing your personnel for the challenges of a real-life attack is just as critical, if not more so, than providing them with the most advanced technologies and systems.

Cyberbit Range is the No. 1 cyber security training platform, providing its users with the ability to build an unlimited supply of high quality cyber security training programs. The courses detailed in this whitepaper present just a few examples of different course types that can be built using Cyberbit Range. Whether you’re looking to build a two-month certification course teaching cyber security from the very beginning, or advanced skill workshops that employers can be enthusiastic about sending their employees to for one day every month.

Cyberbit Range powers dozens of cyber security training centers, academic education centers and business training centers around the world training, qualifying and certifying thousands of students every year.
Range customers speak out

“The shortage in cybersecurity talent and the lack of effective training are proving to be the most pressing industry challenges and a threat to enterprise and national cyber resilience. IABG is proud to bring the most advanced training and simulation platform to Germany to address this gap.”

Prof. Dr. Rudolf F. Schwarz, Managing Director of the IABG Group

“We selected the global leading cyber range platform for our new training center in Tokyo. Based on the success of Cyberbit Range, our customers can expect exceptional quality training, faster certification, and overall more qualified and skilled cyber security personnel.”

Takeshi Mitsuishi, President and CEO, Ni Cybersecurity

“We’ve found Cyberbit Range platform to deliver the highest level of training experience that will enable us to achieve our goals, coupled with the unparalleled support of Cyberbit’s team.”

Dr. Gerson Moreno-Riaño, Executive Vice-President for Academic Affairs, Regent University
ABOUT CYBERBIT™

CYBERBIT’s battle-hardened cybersecurity solutions detect, analyze and respond to the most advanced, complex and targeted threats. A subsidiary of defense systems provider Elbit Systems Ltd. (NASDAQ: ESLT), Cyberbit has more than 500 personnel on three continents helping organizations protect sensitive assets and maximize security operations performance. CYBERBIT solutions empower enterprises to detect advanced threats in seconds, protect critical infrastructure, automate security operations center (SOC) workflows and train staff. With machine learning, big data and continuous technology advancements, Cyberbit maximizes protection against today’s signature-less threats and arms organizations for tomorrow’s new dimension of attack.

www.cyberbit.com | sales@cyberbit.com

Headquarters
22 Zarhin St. | Ra’anana 4310602 | Israel
Tel: +972.(0)9.779.9800

US Office
3800 N. Lamar Blvd. | Suite 200 | Austin, TX 78756
Tel: +1.737.717.0385

EMEA Office
United Kingdom | 103 Kingsway | London WC2B 6QX
Tel: +44.(0)2032.069400

Germany Office
Mies-van-der-Rohe-Str. 8 | 80807 Munich
Tel: +49-89-215416-22

APAC Office
300 Tampines Avenue 5 | #09-02 | Singapore 529653
Tel: +65.6679.5771