CLOUD RANGE

THE NEW STANDARD FOR
CYBERSECURITY PREPAREDNESS

Integrating Experiential Learning in Cyber Curriculum

Debbie Gordon
Founder & CEO
dgordon@cloudrangecyber.com

ABOUT CLOUD RANGE

Cloud Range Manufactures Experience™

Founded in 2018 by Debbie Gordon

Industry's first remotely-delivered cybersecurity simulation training solution

Established a new category in cybersecurity

"Cloud Range has revolutionized cybersecurity training."

- Cybercrime Magazine

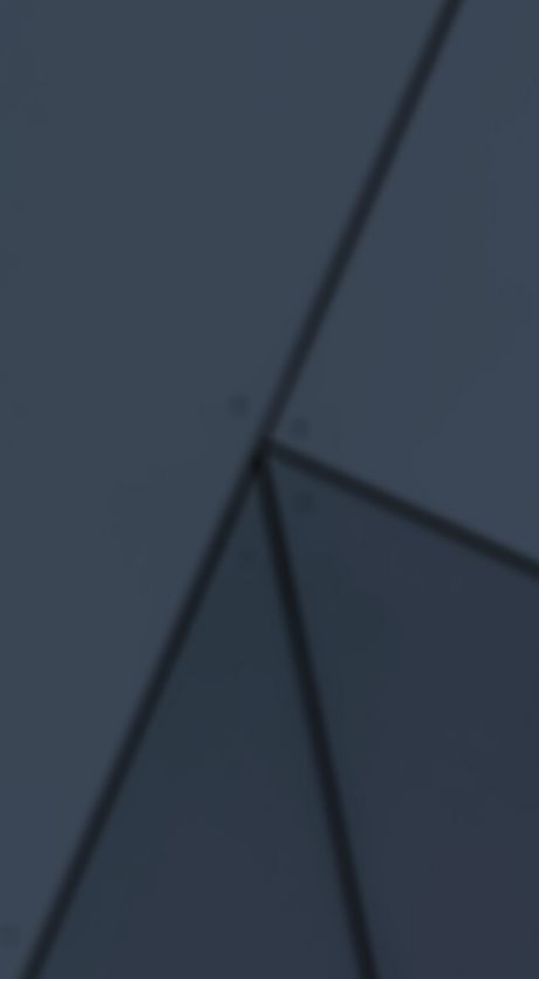
"Cloud Range is ahead of the game."

- Joey Johnson, CISO, Premise Health

Global Presence

Our customers: Enterprise Security Teams, MSSP, Military/Government, Colleges/ Universities, Utilities, Workforce Development

CLOUD RANGE



CYBER SIMULATION IN HIGHER ED IS A NEW CATEGORY.

CLOUD RANGE

WHAT IS A CYBER RANGE/SIMULATION?

Military Roots
Practice Environment
Physical Place
Incident Response Events
Sandbox/Testing Environment
Red Team/ Pen-testing
Product Testing
Cyber Defense Training
Individual Learning Assessments/Reporting

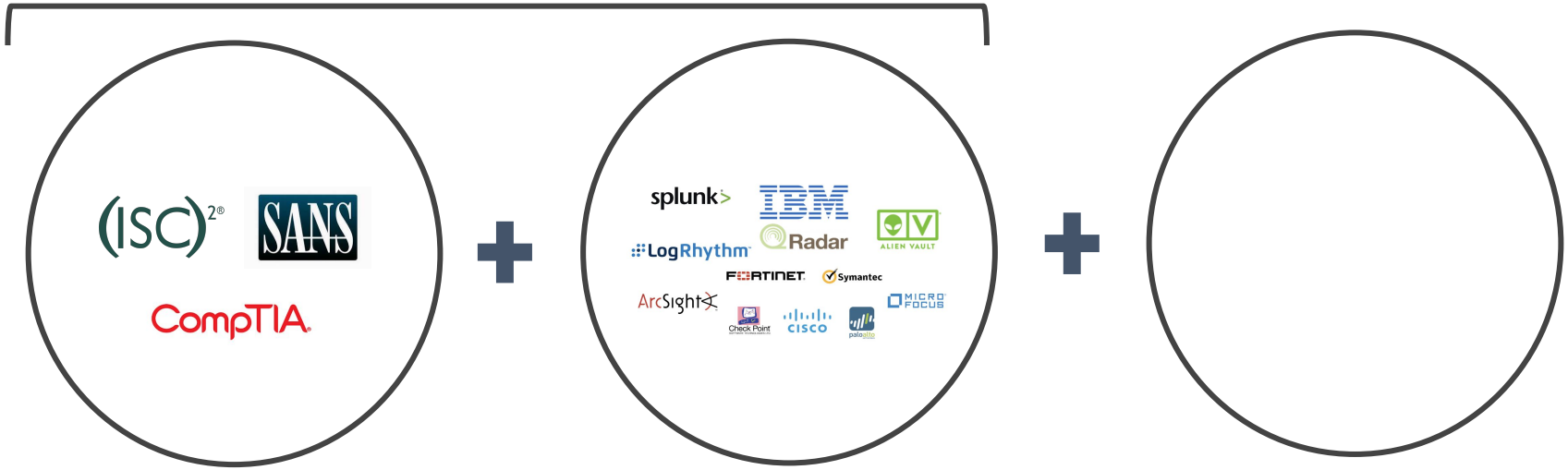
CLOUD RANGE

PROBLEM #1: The Growing Skills Gap

The number of cyber attacks are growing, but there are not enough skilled and experienced **people** to detect and respond to the threats.

CLOUD RANGE

PROBLEM #2: The Experience Gap



Industry certifications, academic certificates and degrees are only theory based

Manufacturer product certifications are only technical (i.e. how to build the engine)

EXPERIENCE HAS BEEN MISSING

"How to fly the plane"

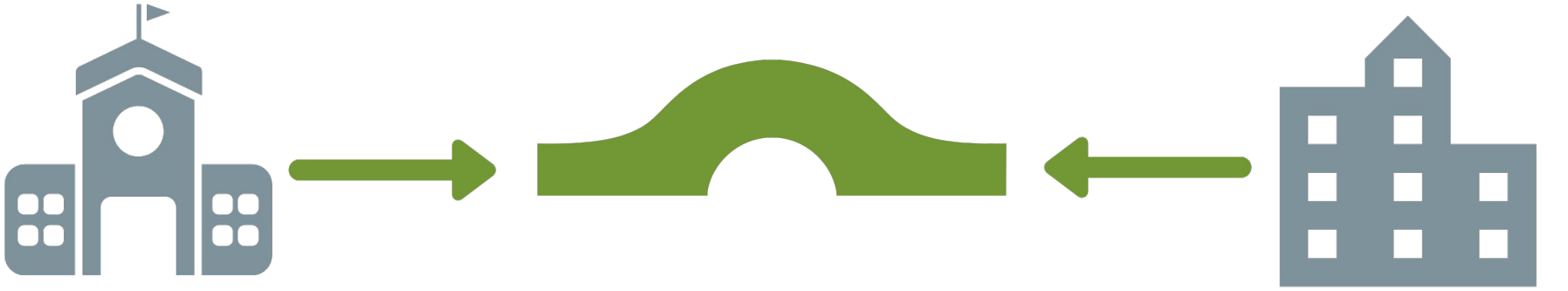
CLOUD RANGE

PROBLEM #3: "On-the-Job" Training is not an Option

Flight simulators give pilots the opportunity to be prepared for every condition when flying. Just like flying a plane, **on the job training is not possible for cyber defenders.**

CLOUD RANGE

PROBLEM #4: The Disconnect



CLOUD RANGE

PROBLEM #5: Cybersecurity changes every day

CLOUD RANGE

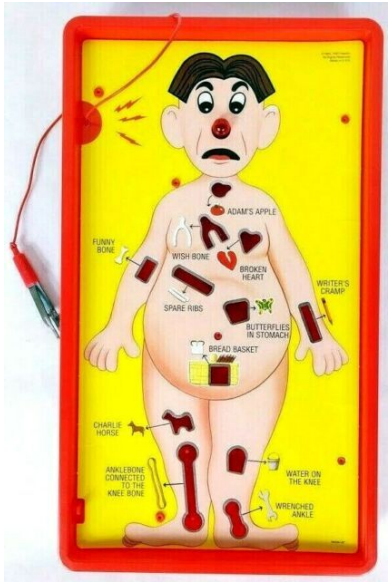
LEARNER SIMULATION LIFECYCLE

CLOUD RANGE

HOW DO WE SOLVE IT?

CLOUD RANGE

WHAT IS SIMULATION?



vs

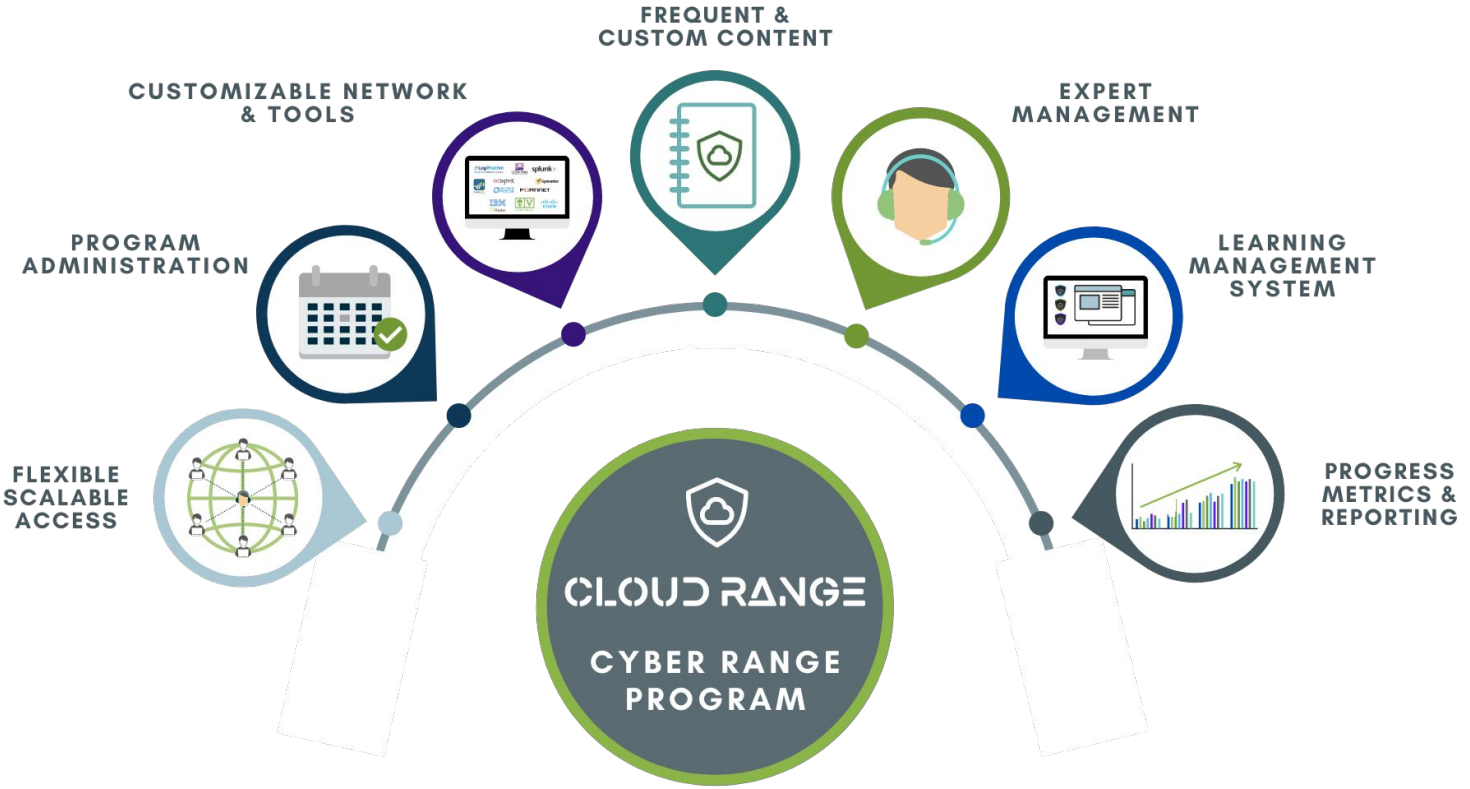
CLOUD RANGE

WHAT IS EFFECTIVE SIMULATION?

VS

CLOUD RANGE

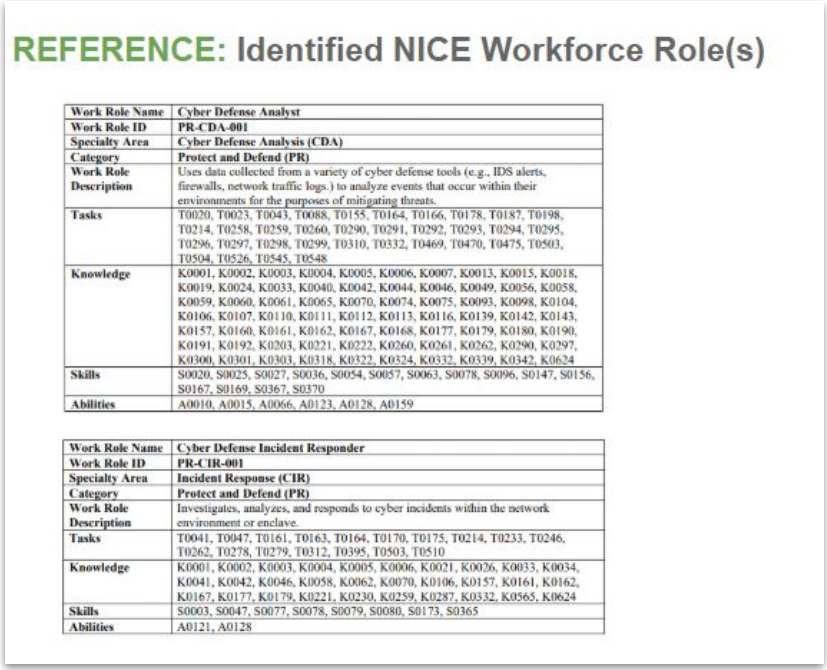
THE ELEMENTS OF A CYBER RANGE PROGRAM?



CLOUD RANGE

Utilizing the NICE Framework

- NICE CyberSecurity Workforce Framework Aligned
- Direct mapping of KSA's to actionable and measured activities



REFERENCE: Identified NICE Workforce Role(s)

Work Role Name	Cyber Defense Analyst
Work Role ID	PR-CDA-001
Specialty Area	Cyber Defense Analysis (CDA)
Category	Protect and Defend (PR)
Work Role Description	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats.
Tasks	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Skills	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Abilities	A0010, A0015, A0066, A0123, A0128, A0159

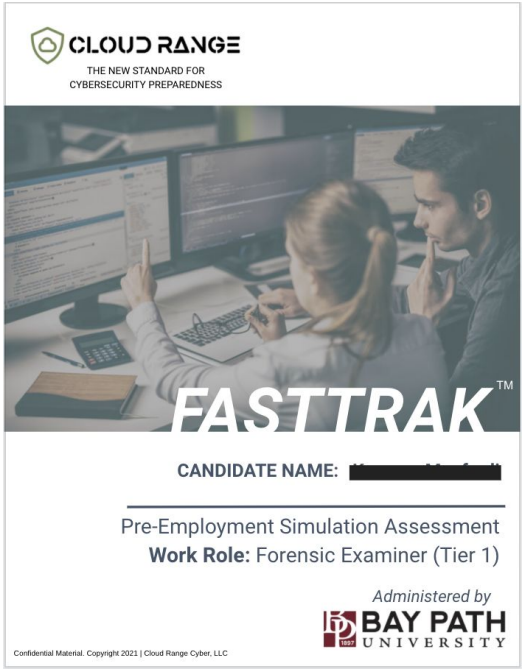
Work Role Name	Cyber Defense Incident Responder
Work Role ID	PR-CIR-001
Specialty Area	Incident Response (CIR)
Category	Protect and Defend (PR)
Work Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Tasks	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624
Skills	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
Abilities	A0121, A0128

CLOUD RANGE

BAY PATH CASE STUDY

BAY PATH UNIVERSITY

Strada EDUCATION NETWORK



CLOUD RANGE

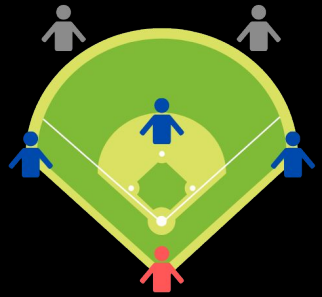
THE SOLUTION

CLOUD RANGE

ELEMENTS OF SIMULATION

TECHNOLOGY

Environment & Tools



PEOPLE

PROCESSES

CLOUD RANGE

ELEMENT OF SIMULATION: TOOLS

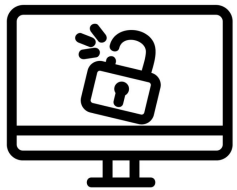
Environment customized to mimic your SOC environment

CLOUD RANGE

EXAMPLE CONTENT

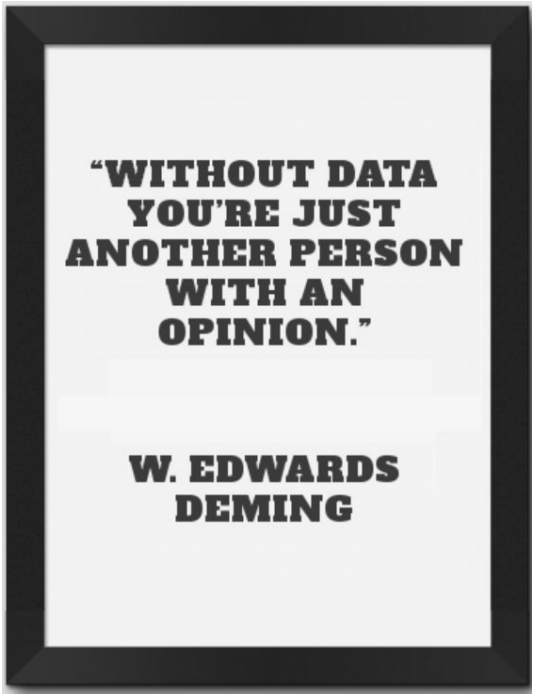
Cyber Attack Scenario Examples

- Apache Shutdown
- Web Defacement
- SQL Injection
- Trojan Data Leak
- Java NMS Kill
- Killer Trojan
- Java Send Mail
- Dragonfly
- Fileless Technique
- DDOS SYN Flood
- Ransomware
- Trojan Share PE
- WMI Worm
- DDOS DNS
- DB Dump via FTP Exploit
- WordPress Blue Bad Plugin
- SQLi Domain Hijacking
- Corporate Espionage
- Supply Chain Attack
- *and more …*



CLOUD RANGE

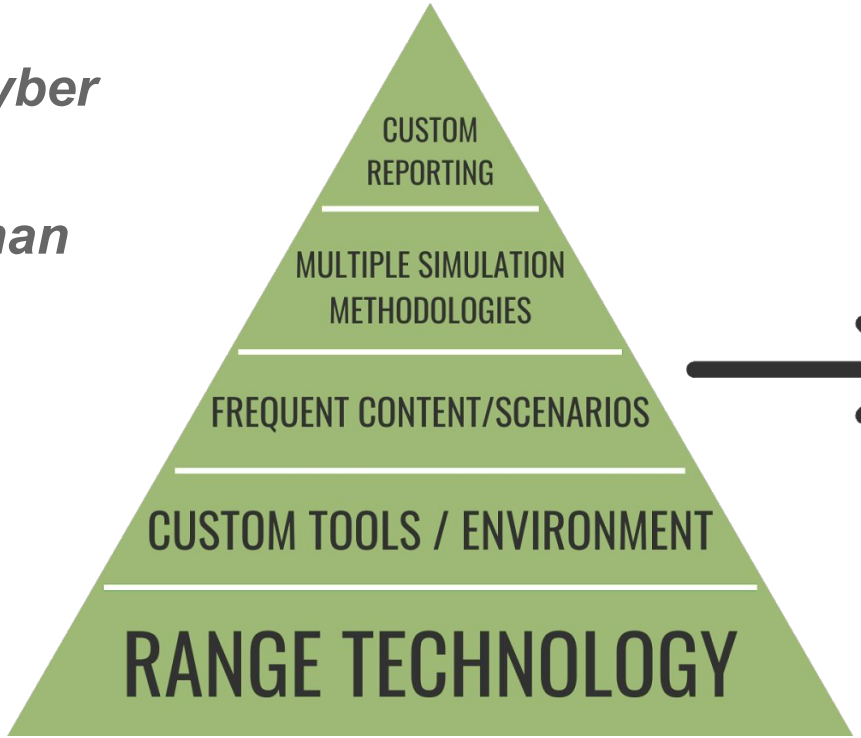
METRICS



CLOUD RANGE

PROGRAM STRUCTURE

"A successful cyber range program requires more than just world-class technology."



OUTCOME

A NEW SECURITY CULTURE: ORGANIZATION-WIDE PROACTIVE & EXPERIENTIAL PREPAREDNESS

CLOUD RANGE

METRICS & REPORTING

CRITICAL SKILL SETS

T0041	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
T0047	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
T00161	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
T00163	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
K0004	Knowledge of cybersecurity and privacy principles
K0005	Knowledge of cyber threats and vulnerabilities.
K0058	Knowledge of network traffic analysis methods
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0397	Knowledge of security concepts in operating systems (e.g., Linux, Unix.)
K0409	Knowledge of cyber intelligence/information collection capabilities and repositories.
K0455	Knowledge of information security concepts, facilitating technologies and methods.
K0471	Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0041	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.
S0170	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).
S0173	Skill in using security event correlation tools
S0192	Skill in auditing firewalls, perimeters, routers, and intrusion detection systems.
S0376	Skill in troubleshooting network equipment (e.g., routers, switches).
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

CLOUD RANGE

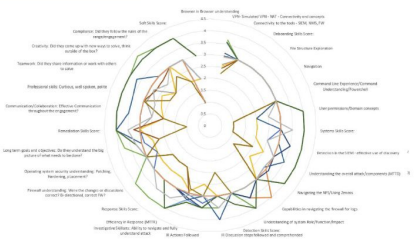
TEAM PERFORMANCE
Scenario: Apache Shutdown

CLOUD RANGE
APACHE SHUTDOWN
LEVEL: NOVICE

Summary

Targeting a known public web server, this scenario emulates an attack on an Apache web server where the attacker uses a Secure Shell (SSH) brute-force attack to gain access to the system. Participants are confronted with a disruption to critical business components and must act swiftly in order to maintain up-time and to mitigate the attack. Participants will learn to detect the attack through the analysis of apache log files, linux system commands and forensics as well as understanding the basics of the attack chain including housekeeping and persistence.

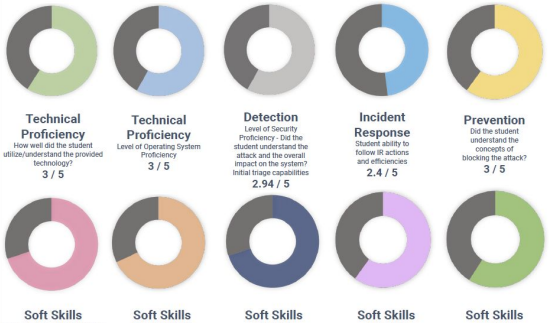
Level	**Novice**
Estimated Time	**2 hours**
Skills Required:	• **Linux log management** • **Apache web server** • **Checkpoint/ Palo Alto firewall** • **ArcSight/ QRadar SIEM**
Overall Score	70-75 - Silver medal



CLOUD RANGE

INDIVIDUAL METRICS

Name: Trainee001
Instructor: Trainer 01
Scenario: **Apache Shutdown**



Overall Comments

Trainee 001 was an excellent leader and well-spoken. He stated near the beginning of the session that the team could improve on their communication/ collaboration and that this would be a priority for them during the session. He called out the initial alarm in ArcSight for password guessing on the Apache server in the DMZ. He began to delegate tasks and ask for occasional status updates from the team. When the password guessing was observed, Trainee 001 stated that they should probably work on blocking that activity and tasked Trainee 008 with this effort. He continued to dig into ArcSight to gather additional details surrounding the suspicious password guessing activity and told the team that it was SSH being targeted. He tasked Trainee 004 with looking into authentication logs on the Apache server. Eventually he also noticed and called out the fact that there were services that had been stopped on the domain controller. He asked the team to log onto the DC to work on identifying any breadcrumbs left by the attacker. Throughout the session Trainee 001 continued to work with the team and put in a solid effort towards keeping things on track. He was taking note of the timeline of events throughout the session which is an important part of incident response. Overall a very solid effort from Trainee 001.

CLOUD RANGE

CLOUD RANGE

BIG PICTURE BENEFITS TO INSTITUTIONS

- Increased employment rate for graduates
- Increased competitive advantage over other institutions
- Market positioning: become the center of a cybersecurity ecosystem
- Ensure curriculum stays current

CLOUD RANGE

CLOUD RANGE

THE NEW STANDARD FOR
CYBERSECURITY PREPAREDNESS

THANK YOU

dgordon@cloudrangecyber.com
www.cloudrangecyber.com