

MN Cyber Range



MN CYBER
RANGE

Train. Test. Detect. Protect.

Who Are We?

Faisal Kaleem

Professor

Metropolitan
State University



DHS/NSA designated CAE-CDE institution

Executive Director



MN CYBER

Train. Test. Detect. Protect

Who Are We?

Corey Blommel

Professor



Trainer



MN CYBER
Train. Test. Detect. Protect

MN Cyber Institute

Statewide Institute for Research and Training in Cybersecurity, Forensics, & IoT

Mission: Position Minnesota as a national leader in cybersecurity through education, innovative public/private partnerships, interdisciplinary research, and community engagement.

Goals:

- Position Minnesota as a national leader in Cybersecurity;
- Create thousands of new high-paying jobs in the state's cybersecurity industry;
- Serve as a statewide facilitator for cybersecurity research and education;
- Enhance Minnesota's cybersecurity workforce, including reintegrating military veterans by utilizing their specialized skills and training;
- Act as a cybersecurity clearinghouse for statewide business and higher education communities;
- Attract new IT, financial, healthcare, transportation, utility and defense companies to Minnesota.

MN CYBER

Train Test Detect Protect

MN Cyber Advisory Board

United Health
Group

Target Corp.

Best Buy

CHS Inc

Ameriprise
Financials

Merrill Corp.

DHS

TCF Bank

Gartner Inc

Ecolab

Protocol 46

RSM US LLC

Deluxe

Corporation

Xcel Energy

3M

MBA

Engineering

State of MN IT
(MN.IT)

Palo Alto
Networks

Elbit Systems

Federal Reserve
Bank of US

US Bank

State Legislators

White Oak Sec

Fairview Services

Azule Foundation

Medtronic

OATI

Maslon LLP

General Mills

Tera Verde Services

Cyber Security Summit

MN Cyber Offerings

- **MN Cyber Range**—A military grade Hyper-realistic simulation and training platform; a first of its kind in the state of MN
- **MN Cyber Academy**—Provider of industry certifications at a nominal cost
- **MN Cyber Pathways**—A collaborative effort to develop a next generation fully immersive cybersecurity curriculum for K-18
- **MN Cyber Residencies**—In-house Cyber Residencies for graduating seniors
- **MN Cyber Placements**—Internship, Apprenticeship and Placement opportunities with in/out state employers via dedicated recruiters
- **MN Cyber Assistantships**—Paid Research Assistantship opportunities for both undergraduate and graduate students to work on exciting projects under Private, State, and, Federal Grants

Cyber related programs at Metropolitan State University

- **Bachelors of Science (BS) in Cybersecurity**
- **Bachelors of Applied Science (BAS) in Computer Forensics**
- BS in Computer Science and Computer Information Technology
- BAS in Information Assurance (offered through MIS)
- **A minor/certificate in Cybersecurity that can be combined with any majors**
- **A minor/certificate in Computer Forensics**
- Master of Science (MS) in Computer Science with concentration in Cybersecurity
- Professional Science Master (PSM) in Computer Science with concentration in Cybersecurity
- A Graduate Certificate in Information Assurance (offered through MIS)
- **A Minor/certificate in E-Discovery**

Plans for 2020 and Beyond

- MS in Cyber Operations—Fall 2020
- 2 Graduate Certificate—Fall 2020
 - Cyber Operations
 - Digital Forensic and Investigations
- Cyber Forensics Research Lab—Fall 2020
- Cyber Residencies with Metro IT—Fall 2020
- MN Civilian Cyber Corp Legislation
- K12 Cyber Initiative
- Establishing more Internship/Apprenticeship
- MN Cyber Physical Space Ready —Spring 2022

What is Cybersecurity?

Cybersecurity has become more than a job

Computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.
- What is Cybersecurity and why it is important? ([Blog](#))



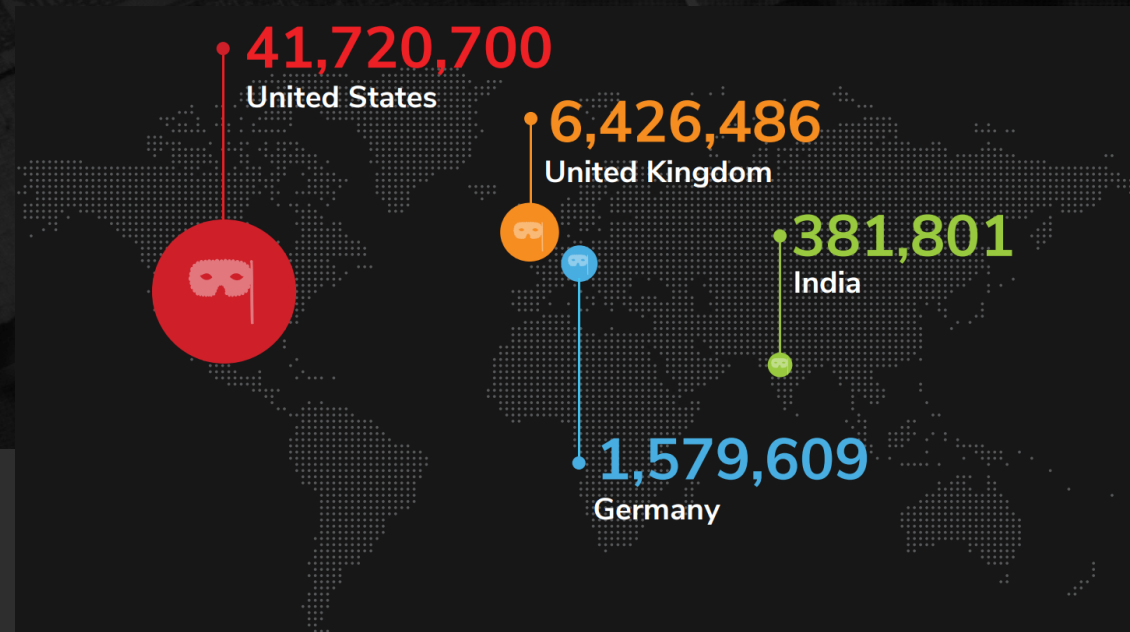
Cyber Threat is real and growing

More than 40 Municipalities have been the victim of cyber attack in 2019

Despite overall declines in malware volume, ransomware continues to pay dividends for cybercriminals. All told, global ransomware volume reached

110.9 Million

for the first half of 2019 — a **15% surge** over the same period last year.



\$1.84 Million

Global average total costs of a

228

Global average days
retailers took to

identify a breach¹



83

Subsequent **days**
retailers then took to

contain it¹

GLOBAL MALWARE ATTACKS

Global average per-record cost
of a retail data breach

YOY INCREASE OF 1.7%¹

Cyber crime will cost the world
6 Trillion USD by 2021

Cyber Security Market Worth
202.36 Billion USD by 2021

2019 Skill Gap Statistics

SKILLS GAP STILL NOT SHRINKING

69%

say their cybersecurity teams are **understaffed**.



58%

have **unfilled (open)** cybersecurity positions.



32%

say it **takes six months or more** to fill cybersecurity jobs at their organization.



TOP 3 REASONS CYBERSECURITY PROS ARE CHANGING JOBS



WANTED: QUALIFIED CANDIDATES

29%

say **fewer than one-quarter** of job candidates are qualified for the cybersecurity position for which they applied

NEARLY 40%

say university graduates in cybersecurity are **not prepared** for the job challenges they'll face

CYBERSECURITY BUDGET GROWTH IS SLOWING



55%

EXPECT AN INCREASE IN CYBERSECURITY BUDGETS

DOWN 9 pts.



1 IN 5

SAY THEIR BUDGETS ARE SIGNIFICANTLY UNDERFUNDED

THE GENDER GAP



15%

say their entire cybersecurity staff is **male**.

51%

say their cybersecurity teams have **significantly more men than women**.

79%

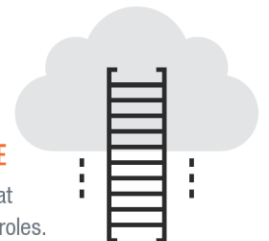
OF MEN SAY MEN AND WOMEN HAVE EQUAL OPPORTUNITIES for career advancement in cybersecurity roles at their organizations.

41%

OF WOMEN AGREE. This number increases to 59% of women among organizations with diversity programs supporting women.

44%

OF ORGANIZATIONS HAVE DIVERSITY PROGRAMS that support women in cybersecurity roles.



Cybersecurity Skill Shortage

Minnesota

TOTAL CYBERSECURITY JOB OPENINGS ⓘ

8,297

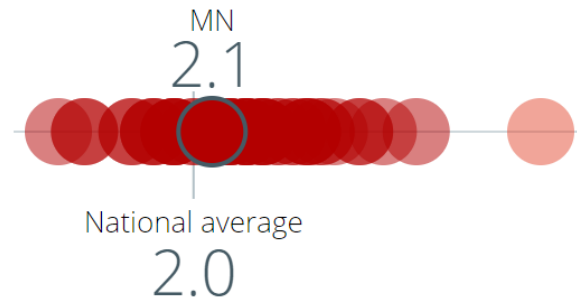
TOTAL EMPLOYED CYBERSECURITY WORKFORCE ⓘ

17,711

SUPPLY OF CYBERSECURITY WORKERS ⓘ

Very Low

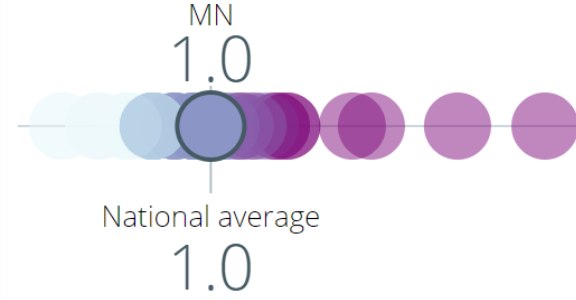
CYBERSECURITY WORKFORCE
SUPPLY/DEMAND RATIO



GEOGRAPHIC CONCENTRATION ⓘ

Average

LOCATION QUOTIENT



TOP CYBERSECURITY JOB TITLES ⓘ

- Cyber Security Engineer
- Cyber Security Analyst
- Vulnerability Analyst / Penetration Tester
- Cyber Security Consultant
- Network Engineer / Architect
- Systems Engineer
- Cyber Security Manager / Administrator
- Software Developer / Engineer
- Risk Consultant

Global Training Crisis | Some Stats



62%

of cybersecurity execs say that **lack of skilled staff is their #1 security operations challenge**

SANS SOC Survey 2019



61%

Of employers say that **most cybersecurity applicants are not qualified**

ISACA State of Cybersecurity, 2017



62%

of cybersecurity professionals say their organization is **not providing an adequate level of training** to keep up with risks

The life and times of cybersecurity professionals
ESG and ISSA, 2017



45%

of employers believe that most applicants **don't understand the business of cyber security**

ISACA State of Cybersecurity, 2017

Training Challenges

What Our Customers Have to Contend with

Training Does Not Prepare for the Real World

Tabletops, SANS courses, and red vs. blue exercises do not deliver a real-world cyberattack experience

Training Logistics

Registration, travel, coordinating team schedules. You can't train whenever you want

Training is Focused on Operating Tools

Neglecting critical skills such as communication, and performance under pressure

Hard to Prepare for Advanced Threats

Red teams hired to train blue teams often cannot replicate the capabilities of sophisticated attackers

Lack of Teamwork Training

Limited options to develop critical communication and collaborative skills



MN CYBER
RANGE

Train. Test. Detect. Protect.

Introducing MN Cyber Range

The “Flight Simulator” for Cybersecurity

The First Hyper-Realistic Cybersecurity Training Platform



CYBERBIT
PROTECTING A NEW DIMENSION

Elbit Systems
of America

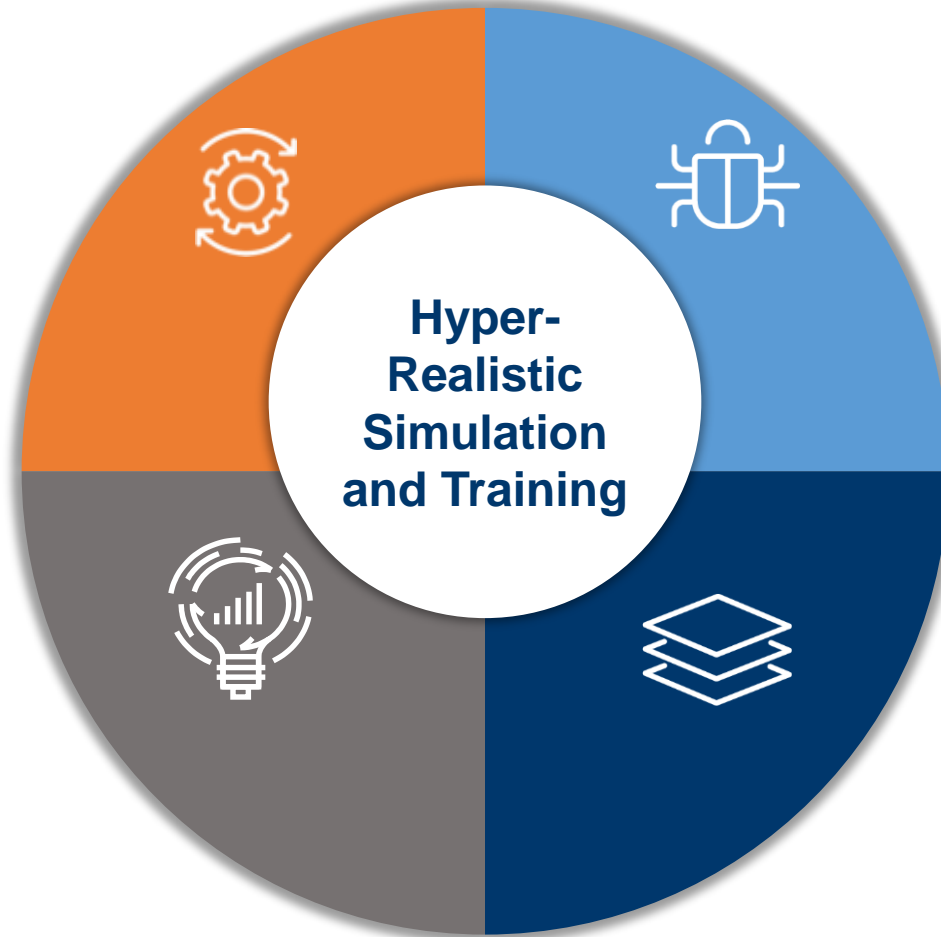
The Principles of Hyper-Realistic Cyberattack Simulation

Real-World Network

Mirroring a comprehensive corporate network

Real-World Tools

Market Leading security tools, as in a real-world SOC



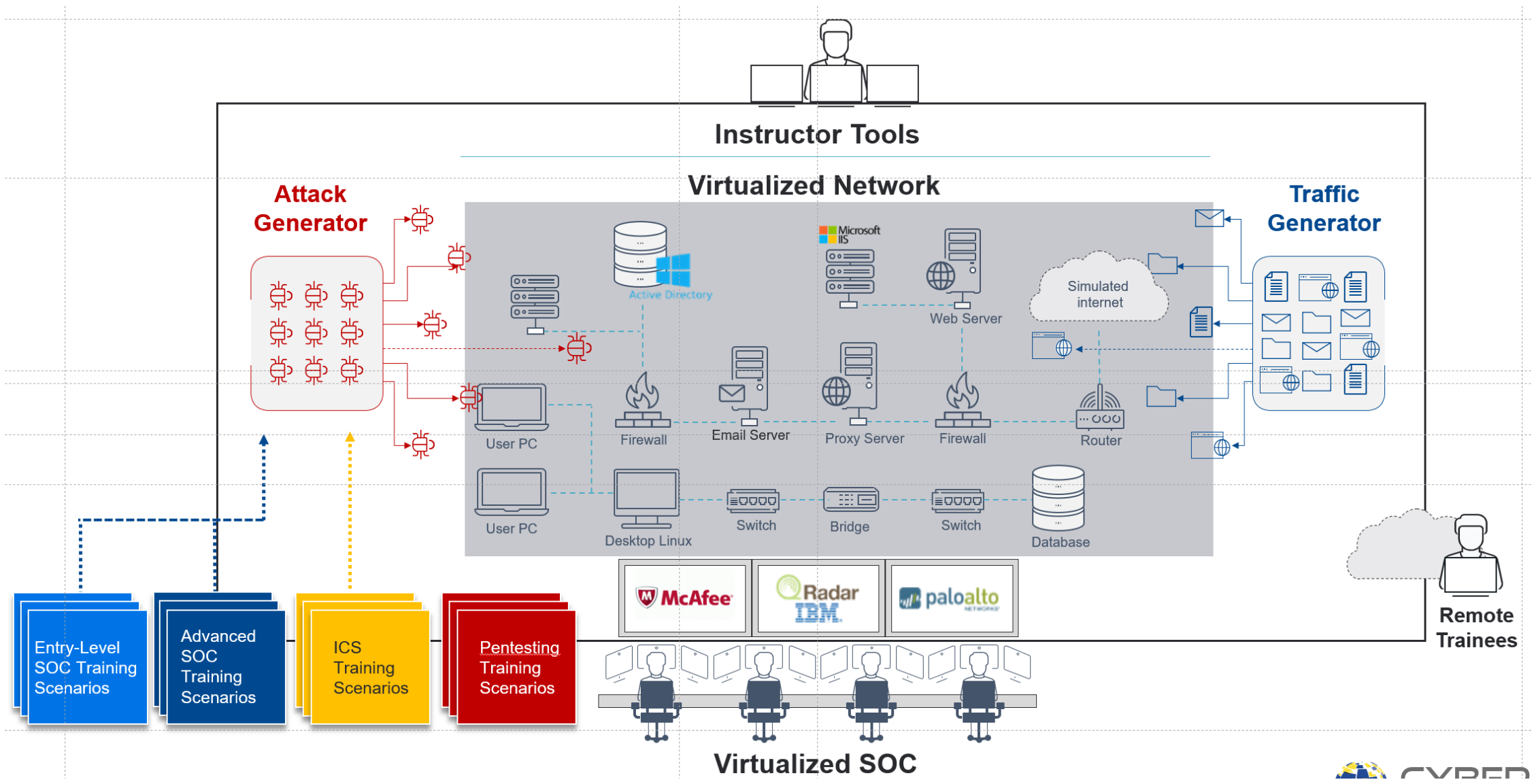
Real-World Attacks

Automated, simulated attacks based on real-world scenarios

Tracking and Feedback

Recording, debrief, predefined goals, automated trainee assessment

The Cyber Range Platform



Diverse Use Cases and Scenarios



Multiple Roles

- Tier-One Analyst
- Tier-Two Analyst
- SOC Manager



Diverse Scenarios

- Individual or team
- Entry level to advanced, evasive attacks
- Multiple Attack Types: DDoS, Defacement, Ransomware, Trojans and more...



Multiple Use Cases


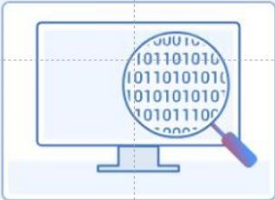


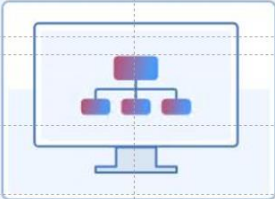




- Individual Skill Development
- Team Training
- Onboarding New Members
- Candidate Assessment
- Playbook Testing

MN Cyber Range Features and Courses

- On-Premise or Remote Capability
- Automatic Scenario Emulator
- Training focused on improving Individual and Team Skills
- Ability to plug-in other tools on a subnet
- Off-the-Shelf Content
- Content Creation Tools
- Support for IT and OT Environments



MN Cyber Range Training Options

	Tier 1 SOC Analysis		Tier 2 SOC Analysis		Advanced Incident Response
	Malware Analysis		Network Forensics		Industrial Control Systems
	Penetration Testing		Windows Forensics		Linux Forensics

Detailed briefing; goals and guidelines

The screenshot displays the CyberBit interface for the 'Apache Shutdown' attack scenario. The interface includes a navigation bar with 'HOME' and 'Tier 1 SOC Analysis', and a sidebar with 'Attack Scenarios' and a search bar. The main content area is titled 'Apache Shutdown' and features a 'RUN' button. The scenario details are as follows:

- Description:** This scenario emulates an attack on the organizational publicly-accessible services. The attack disrupts the operation of the service and utilizes basic methods to strengthen the attacker's foothold in the system. In this scenario, the trainees are confronted with a disruption to business critical components and need to act swiftly in order to maintain as much up-time as possible.
- Difficulty Level:** Medium (indicated by a gauge).
- Estimated Duration:** 03:00 Hrs.
- Objectives:**
 - ★ Practicing Linux and Apache logging research and basic forensics
 - ★ Gaining hands-on experience with Apache, SSH client, and Linux management tools
 - ★ Gaining hands-on experience with an event of brute-force attack
- Recommended Skill Set:**
 - Linux log management (checked)
 - Apache web server (checked)
 - Firewall (checked)
 - SIEM (checked)
- Attack Flow:**
 - 1 Port Scanning
 - 2 SSH Brute Force Attack
 - 3 Stop Apache Services
 - 4 Create Backdoor Scripts
- Network:** A diagram of an IP Network showing various nodes and connections.

Comprehensive Network

CYBERBIT Cyber Range 3.5.11 Demo - Class 1

< HOME | Settings

Students Stations Scenarios Networks

Networks

+ Add Network

Search

IP Network

IP Network 2

IP Network with EDR solution

Malware Analysis Network 1

Malware Analysis Network 2

Red Network 1

Red Network 2

IP Network

A Medium IP network with a DMZ, Several Servers and 5 Workstations

The diagram illustrates a comprehensive network architecture. At the center is a core router (CNT-FW) with IP 192.168.254.241/29. It connects to several VLANs:

- Server Segment (192.168.200.X, VLAN 2000):** Includes servers like CNT-SNORT, CNT-DC, CNT-DB, CNT-OSX, CNT-CM, CNT-Zenoss-NMS, CNT-EPO, CNT-Mail, CNT-FW5, CNT-DHCP, CNT-Files, and CNT-MySQL.
- Web Segment (192.168.213.X, VLAN 2002):** Includes CNT-Web-ProfTFTP, CNT-Web-IP, and CNT-Web-IP5.
- DMZ Segment (172.16.100.X, VLAN 2011):** Includes various DMZ servers like CNT-DMZ-IP2, CNT-DMZ-IP1, CNT-MailRelay, CNT-DMZ-DNS, CNT-DMZ-Proxy, CNT-DMZ-APACHE1, CNT-DMZ-APACHE2, and CNT-DMZ-APACHE3.
- SIEM Segment (192.168.66.X, VLAN 2008):** Includes AnSight and AnSight-Col.
- User Segment (192.168.100.X, VLAN 2005):** Includes WS-Ubuntu-Cnt1, WS-Ubuntu-Cnt2, WS-Win7-Cnt1, and WS-Win7-Cnt2.
- DB Segment (192.168.214.X, VLAN 2004):** Includes CNT-DB-MYSQL, CNT-DB-SQL, CNT-DB-Postgrez, and CNT-DB-Postgre1.
- InterConnect Segment (192.168.254.X, VLAN 2009):** Includes SCA-OpenVPN, SCA-HMI, SCA-L3, and SCA-L3-R.
- SCADA Segment (12.8.201.X, VLAN 2008):** Includes SCA-PLC01 and SCA-PLC02.
- VPN Segment (192.168.110.X, VLAN 2012):** Includes a Training & Management segment.
- Custom Segment (192.168.56.X, VLAN 2056):** Includes Internet Web, Internet-Mail, Internet-MYSQL, Internet-DNS, and Internet-WebMail.

Physical Layer devices include SCA-PLC01, SCA-PLC02, SCA-PLC01, and SCA-PLC02.

Ongoing Recording, Playback and Goal Tracking

CYBERBIT Cyber Range 3.5.11 Demo - Class 1

< HOME | SOC day1

Active Scenario: Apache Shutdown | 00:00:52 | Total Score: 0/100

Observer | Traffic Generator | Network

Attack Scenarios

- Apache Shutdown**
 - Set Timer | See Guides
 - Detection
 - Detect a new port scanning incident
 - Detect a successful password brute force attack
 - Detect failure of Apache services
 - Analyze the reasons for the Apache services failure
 - Response
 - Prevention
- DB Dump via FTP Exploit**
 - Set Timer | See Guides
 - Detection
 - Response

Students

- Ashley Robinson** - Junior SOC Analyst
- Daniel Thompson** - Malware Analyst
- Donald Jackson** - Malware Analyst
- Edward Adams** - Senior SOC Analyst

Ashley Robinson Evaluation

Ashley Robinson Evaluation | Overall Rating: ★★★★★

Comment: Add Comment

Professional skills: ★★★★★
Teamwork skills: ★★★★★
Compliance: ★★★★★
Total: ★★★★★

Training Timeline: 00:03 | 00:18 | 00:33 | 00:48 | 01:03 | 01:18 | 01:33 | 01:48 | 02:03 | 02:18 | 02:33 | 02:48 | 03:03 | 03:18 | 03:33 | 03:48 | 04:03 | 04:18 | 04:33 | 04:48

Automated Assessment

The screenshot displays a security training interface for Sheldon Cooper, SOC operator. The interface includes a top navigation bar with 'Get Help', 'Hint', 'Full Solution', 'Training Time 00:21:32', and a 'STOP TRAINING' button. Below the navigation bar, there are tabs for 'Investigation', 'Network Info', 'Network Map', 'Collaboration', and 'Quiz'. The main area shows a timeline of events with icons for 'Port Scan', 'Brute Force', and 'Malicious File..'. A yellow callout box highlights the 'Automated Grading of Collected Evidence' feature. Below the timeline is a table of collected evidence items.

CREATED BY	ATTACK TYPE	EVIDENCE DESCRIPTION	ATTACK TIME	FOUND AT	ACCURACY
Sanda	Process	SIEM Message: (Elbit) -	10:14:30	11:14:30	3/5
Sanda	Process	SIEM Message: (Elbit) -	10:14:30	11:14:30	3/5
Sanda	Process	SIEM Message: (Elbit) -	10:14:30	11:14:30	3/5
Sanda	Process	SIEM Message: (Elbit) -	10:14:30	11:14:30	3/5

Automated Assessment

Knowledge Quiz to Complement Hands-On Training

The screenshot displays a training interface for a 'Trainee 01' (SOC Operator). The top navigation bar includes 'Get Help', 'Hint', 'Solution Brief', 'Training Time' (00:00:10), and a 'COMPLETE TRAINING' button. The main content area is divided into two sections: an 'Investigation Quiz' on the left and an 'End of Training' modal on the right.

Investigation Quiz

Answer the questions as you go. Your answers will be evaluated as you complete the training.

1. Who knows the root password?
 - the password is known to all
 - the password is known to the attacker
 - only the attacker knows the password
 - the password was compromised
2. What can be done to prevent a password from being compromised?
 - block all traffic from the attacker
 - block all connections to the server
 - Prevent ssh connections to the server
 - Update the Apache server
3. what is the best practice for password management?
 - users should change their passwords frequently
 - The domain administrator should change the passwords
 - Users should change their passwords frequently
 - the passwords should be long and complex

End of Training

Dear trainee, The training has been completed

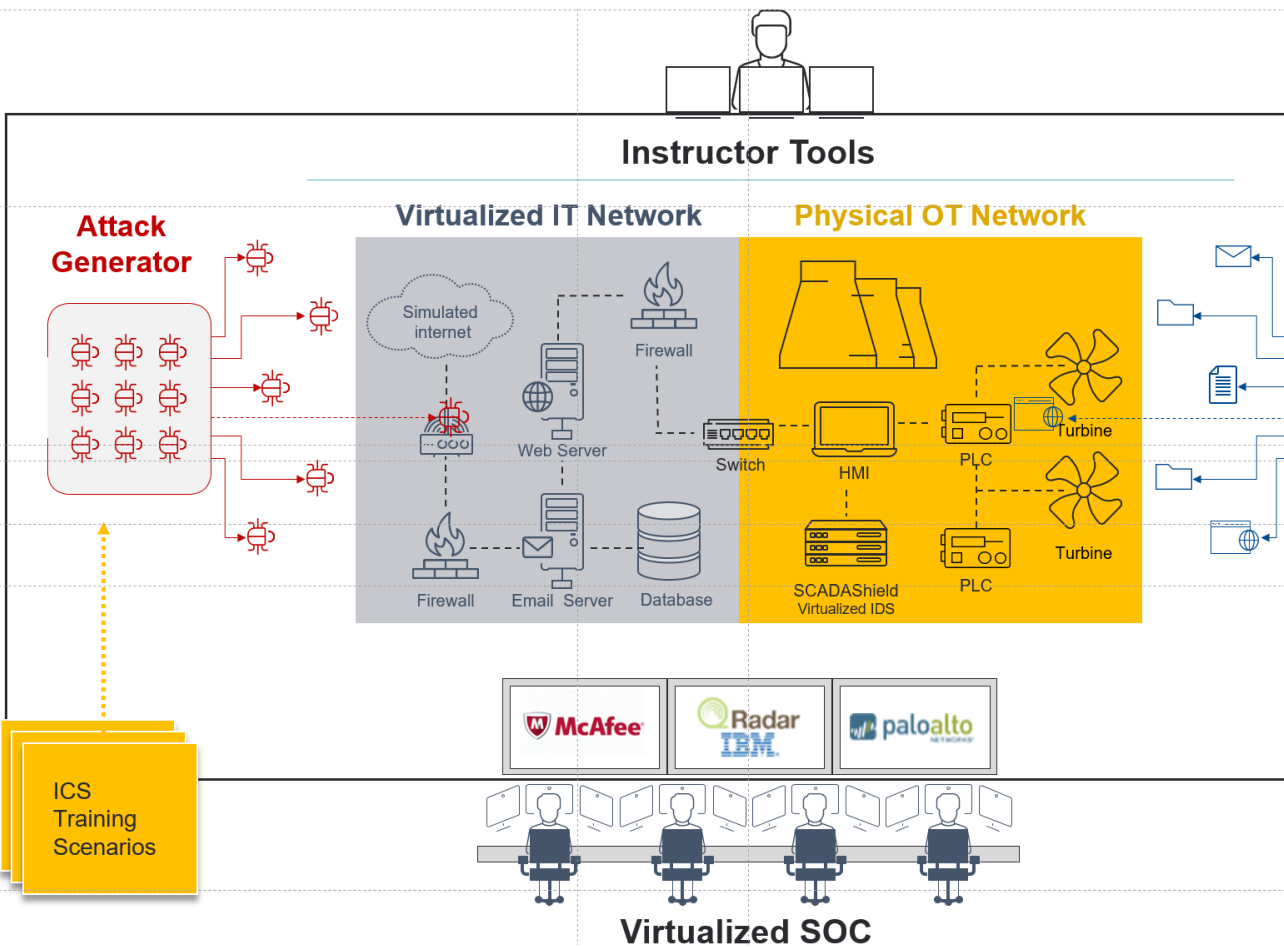
Thanks for taking part in this session, see you next time!

OK, Bye Bye!

SUBMIT

ICS Training

Real World OT Controllers, IT/OT Attacks



Training Info

Training: New Training

Scenario: DB Dump via FTP Exploit

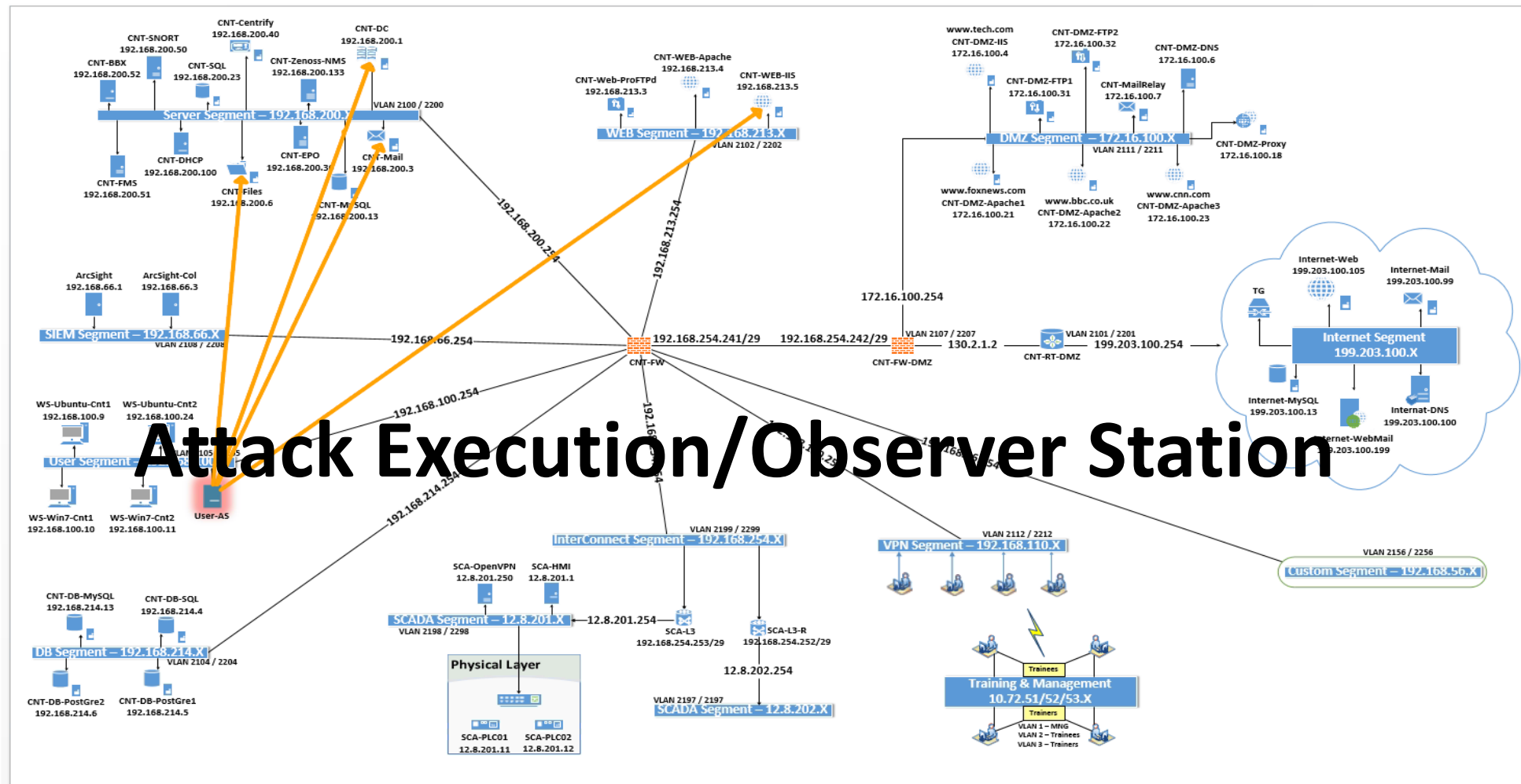
Blue team members: 4

TG status: ●

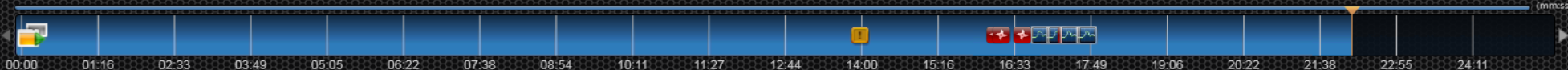
Network status: ●

Training Activity

Port Scan Started	00:16:20
Port Scan Started	00:16:41
Rule: Port scanning Detected-Port scanning detected from:192.168.100.64 to:192.168.213.3	00:16:59
Rule: Port scanning Detected-Port scanning detected from:192.168.100.64 to:192.168.213.4	00:17:14
Rule: Port scanning Detected-Port scanning detected from:192.168.100.64 to:192.168.213.5	00:17:16
Http Crawler Started	00:17:25
Rule: Port scanning Detected-Port scanning detected from:192.168.100.64 to:192.168.200.1	00:17:28
Rule: Port scanning Detected-Port scanning detected from:192.168.100.64 to:192.168.200.3	00:17:44
Rule: Port scanning Detected-Port scanning detected from:192.168.100.64 to:192.168.200.6	00:17:46



Http Crawler Started



MN Cyber Physical Space



Other Available Resources

Nationally recognized faculty & Researchers

Access to industry experts in the form of community faculty

Dedicated labs and equipment for cybersecurity, forensics, IoT research and training

Powerful Virtual Infrastructure



Contact Info

Faisal Kaleem

Faisal.Kaleem@metrostate.edu

651-793-1238

LinkedIn: Kaleemf

Twitter: @Kaleemf

www.metrostate.edu

www.mncyber.org

info@mncyber.org

Corey Blommel

Corey.Blommel@anokaramsey.edu

763-433-1154

LinkedIn: corey-blommel-437829a

www.anokaramsey.edu/

Thank You

Questions

Metropolitan
State University



DHS/NSA designated CAE-CDE institution



MN CYBER

Train. Test. Detect. Protect