NISTCSF.COM

NIST Cybersecurity Framework (NCSF)

Workforce Development Solutions

itSM Solutions℠

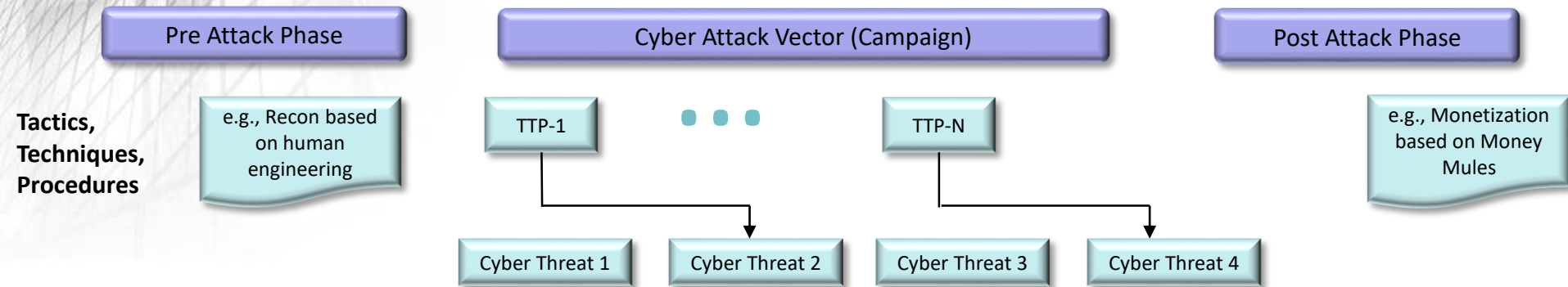IT Experience. Practical Solutions.

AGENDA

- The Cybersecurity Threat Landscape

- The Business Cybersecurity Challenge

- NIST Cybersecurity Framework

- NICE Cybersecurity Workforce Framework

- Introduction to NISTCSF.COM

- The NCSF Controls Factory Methodology

- NCSF Training Programs
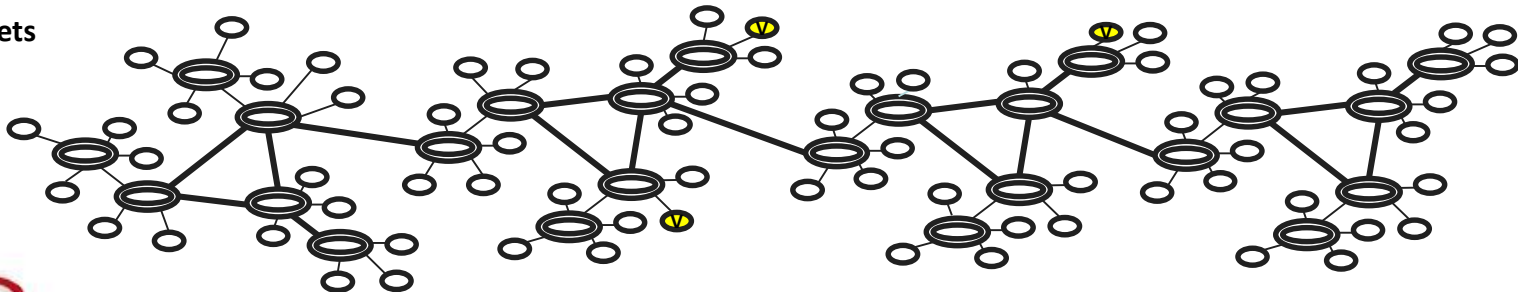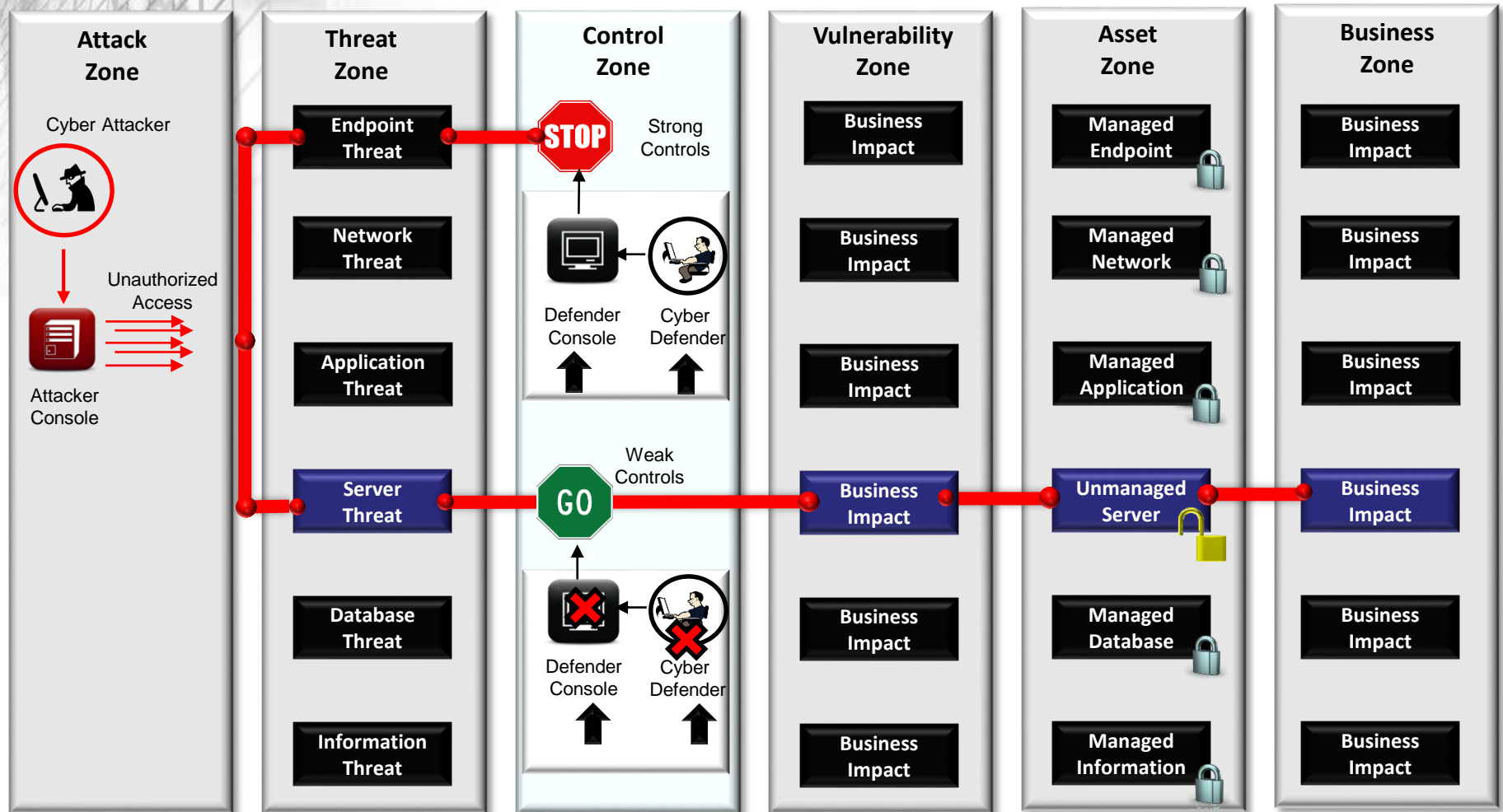
The Cyber Threat Landscape

Cyber Attack Campaigns

Pre Attack Phase	Cyber Attack Vector (Campaign)	Post Attack Phase

Tactics, Techniques, Procedures

e.g., Recon based on human engineering

TTP-1 • • • TTP-N

e.g., Monetization based on Money Mules

Cyber Threat 1	Cyber Threat 2	Cyber Threat 3	Cyber Threat 4

Cyber Kill Chain

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Action on Objectives

NIST CSF

Identify	Protect	Detect	Respond	Recover

Affected Assets

itSM Solutions
IT Experience. Practical Solutions.

Modeling the Zones of Cyber-Attacks

Attack Zone	Threat Zone	Control Zone	Vulnerability Zone	Asset Zone	Business Zone
Cyber Attacker	Endpoint Threat	Strong Controls	Business Impact	Managed Endpoint	Business Impact
Unauthorized Access	Network Threat	Defender Console / Cyber Defender	Business Impact	Managed Network	Business Impact
Attacker Console	Application Threat		Business Impact	Managed Application	Business Impact
	Server Threat	Weak Controls	Business Impact	Unmanaged Server	Business Impact
	Database Threat	Defender Console / Cyber Defender	Business Impact	Managed Database	Business Impact
	Information Threat		Business Impact	Managed Information	Business Impact

The Business Cybersecurity Challenge
Recruiting, Training & Skilling a NIST/NICE Cybersecurity Workforce
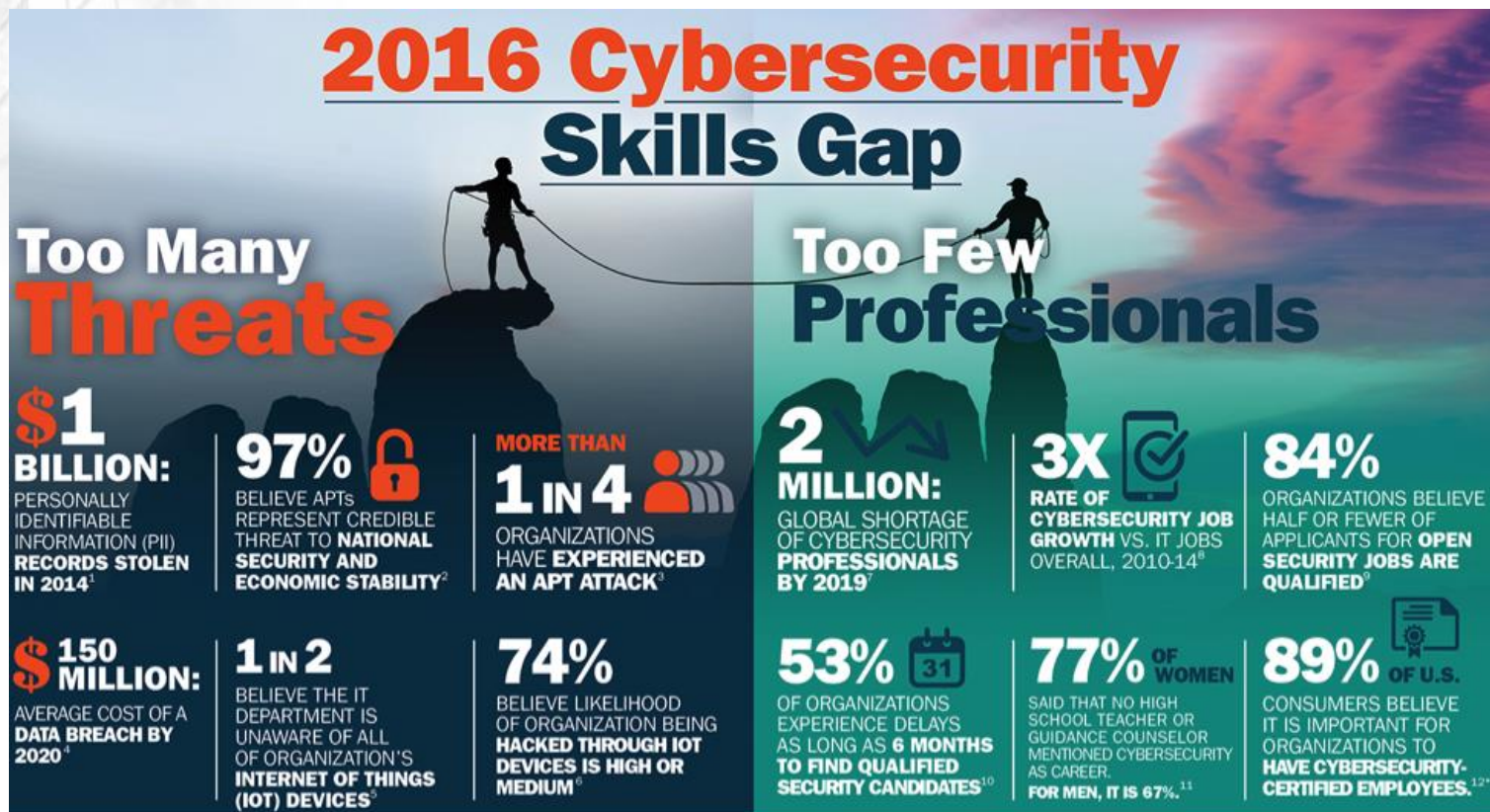
NIST Cybersecurity Framework (NCSF)

- Published by the
  - National Institute of Standards & Technology (NIST)
    - Department of the U.S. Department of Commerce
    - Published February 2014
    - Deemed appropriate for organizations worldwide
    - Mandatory for Federal Agencies per EO May 2017
- Risk-based approach
  - Manages cybersecurity risk
  - Framework Core
    - Describes common desired outcomes
    - Expressed as functions
  - Framework Implementation Tiers
    - Describes how cybersecurity is practiced
    - Informed by business needs
  - Framework Profiles
    - Aligns "core" with resources & tolerances
    - Used to define current state
    - … & future state

———————

"The framework is intended for organizations that are responsible for critical infrastructure, defined as 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety…'"

———————

NIST
National Institute of
Standards and Technology

itSM Solutions℠
IT Experience. Practical Solutions.

NIST/NICE Cybersecurity Workforce Framework (NCWF)

- The NIST/NICE Cybersecurity Workforce Framework (NCWF) was released in November of 2016

- NCWF provides a common language to categorize and describe NCSF work and specialty roles

- NCWF was designed to serve several key groups, including employers, candidates, educators, trainers and technology providers.

- NCWF provides details on the knowledge, skills, abilities and credentials required to perform NCSF work and specialty roles

- NCWF provides an online app called Cyberseek to help candidates find a job in their area of study

NICE Cybersecurity Workforce Framework (NCWF)

No.	NCWF Category	Category Description	Related CSF Functions
1	Securely Provision (SP)	Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.	Identify (ID) Protect (PR)
2	Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	Protect (PR) Detect (DE)
3	Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	Identify (ID) Protect (PR) Detect (DE) Recover (RC)
4	Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	Protect (PR) Detect (DE) Respond (RS)
5	Analyze (AN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	Identify (ID) Detect (DE) Respond (RS)
6	Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	Detect (DE) Protect (PR) Respond (RS)
7	Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	Detect (DE) Respond (RS) Recover (RC)

NISTCSF.COM

- **NISTCSF.COM** is a NIST Cybersecurity Framework (NCSF) workforce development program brought to you by itSM Solutions LLC and UMass Lowell a NSA/DHS National Center of Academic Excellence in Cyber Defense Research (CAE-R).

- This innovative, cybersecurity workforce development program is built around an NCSF Controls Factory™ model created by Larry Wilson, the CISO in the university president's office.

- The itSM/UMass program teaches individuals and organizations the knowledge, skills and abilities to engineer, operate and govern a cybersecurity program based on the NIST Cybersecurity Framework

- The NCSF program and its author have won many industry awards including:
  - Security Magazine most influential cyber security professionals North America, 2016
  - SANS Person who made a difference in Cybersecurity, 2013
  - Information Security Executive (ISE) nominee for Executive of the Year for North America, 2013
  - ISE North America Project Award Winner I for the Academic and Public Sector 2013

The NCSF Controls Factory

- The UML NCSF Controls Factory methodology is an easy to understand approach to operationalizing the NCSF across an enterprise and its supply chain
- The controls factory methodology helps enterprises of any size learn how to engineer, test, operate and improve the technical and business functions of a NCSF program
- The program is completely adaptable to any framework or standard and can easily be updated, replaced or modified with minimal impact to the overall solution.

The Controls Factory Model
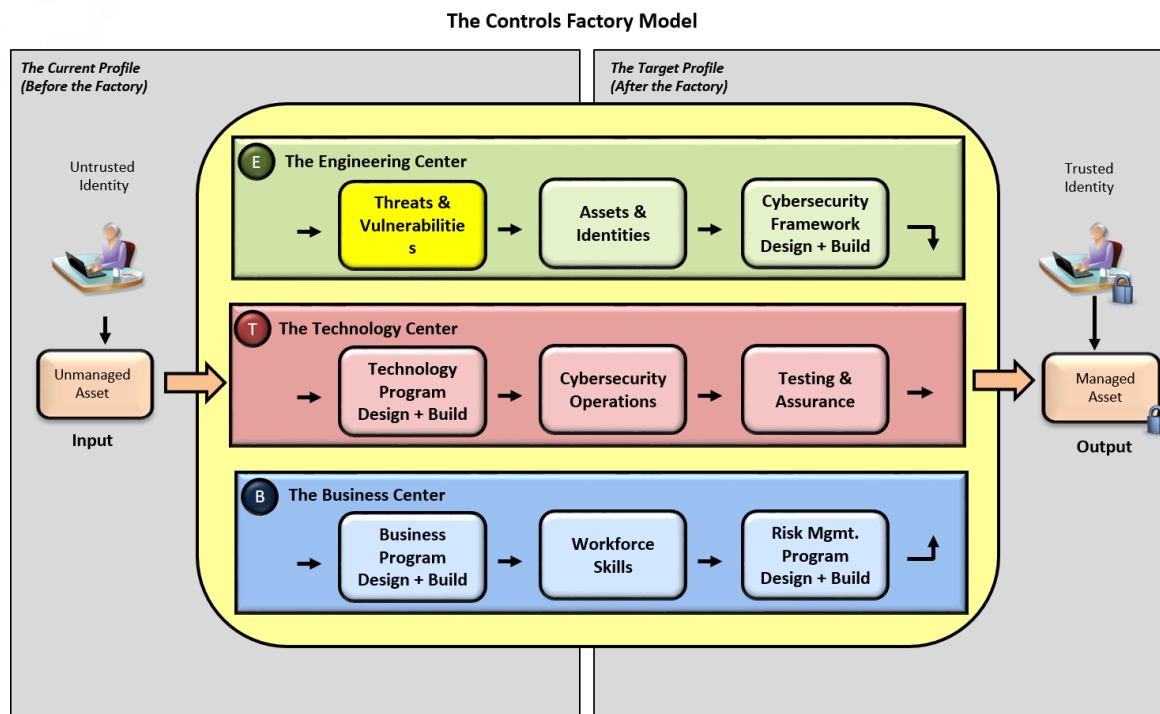
NCSF Workforce Training Tracks
Learning NCSF Knowledge, Skills & Abilities

NCSF-CFM Engineering Track
NCSF Controls Focus

Delivery:
- **Online, Classroom, Self-Study and Blended with Simulations & Labs**

Curriculum:
- **NCSF-CFM Certification Trainings**
- **NCSF-ENG Certification Trainings**
- **NCSF-NICE Certification Trainings**
- **IT Certification Trainings**
- **ITSM Certification Trainings**
- **AGILE Certification Trainings**
- **Business Skill Trainings**

NICE Workforce Category:
- **Securely Provision**
- **Analyze**

NCSF-CFM Technical Track
NCSF Operations Focus

Delivery:
- **Online, Classroom, Self-Study and Blended with Simulations & Labs**

Curriculum:
- **NCSF-CFM Certification Trainings**
- **NCSF-TEC Certification Trainings**
- **NCSF-NICE Certification Trainings**
- **IT Certification Trainings**
- **ITSM Certification Trainings**
- **AGILE Certification Trainings**
- **Business Skill Trainings**

NICE Workforce Category:
- **Operate and Maintain**
- **Protect and Defend**
- **Collect and Operate**

NCSF-CFM Business Track
NCSF Governance Focus

Delivery:
- **Online, Classroom, Self-Study and Blended with Simulations & Labs**

Curriculum:
- **NCSF-CFM Certification Trainings**
- **NCSF-BUS Certification Trainings**
- **NCSF-NICE Certification Trainings**
- **IT Certification Trainings**
- **ITSM Certification Trainings**
- **AGILE Certification Trainings**
- **Business Skill Trainings**

NICE Workforce Category:
- **Oversee and Govern**
- **Investigate**

Note: The above NCSF training tracks can function as a standalone training solution or be integrated into a two or four year higher education degree program

NCSF Foundation Certification

NCSF Foundation Certification Training

- The NCSF Foundation training course outlines current cybersecurity challenges and explains how organizations who implement a NCSF program can mitigate these challenges.

- This program is focused on candidates who need a basic understanding of NCSF to perform their jobs as Executives, Business and Information Technology (IT) professionals.

  - **Location of Training:** Onsite or Online
  - **Means of Instruction:** Classroom, Virtual Classroom & Self Paced Video
  - **Number of Classroom Hours: 12 (1 Day)**
  - **Optional NCSF Simulation Game (1/2 Day)**
  - **Prerequisites:** None
  - **Credentials Attained:** Certification, College Credits, PDU's & CEU's

NCSF Practitioner Certification

NCSF Practitioner Certification Training

- The NCSF Practitioner training course teaches in detail how to engineer, operate and improve the technical and business functions of an NCSF program.

- This program is focused at existing cybersecurity professionals who want to learn the knowledge, skills and abilities to work as Engineers, Operators and Risk Governance professionals in an NCSF program.

  - **Location of Training:** Onsite or Online
  - **Means of Instruction:** Classroom, Virtual Classroom & Self Paced Video
  - **Number of Classroom Hours: 30 (4 days)**
  - **Prerequisites:** NCSF Foundation Certification
  - **Credentials Attained:** Certification, College Credits, PDU's, CEU's

NCSF Boot Camp Certification

NCSF Boot Camp Training

- This combined NCSF program outlines current cybersecurity challenges plus teaches in detail how to engineer, operate and improve the technical and business functions of a NCSF program.

- This program is focused on **new cybersecurity candidates** who need to understand current cybersecurity challenges plus a detailed understanding of NCSF to perform their daily roles as Engineers, Operations and Risk Governance cybersecurity professionals.

  - **Location of Training:** Onsite or Online
  - **Means of Instruction:** Classroom, Virtual Classroom & Self Paced Video
  - **Number of Classroom Hours: 32 (5 days)**
  - **Credentials Attained:** Certification, College Credits, PDU's, CEU's
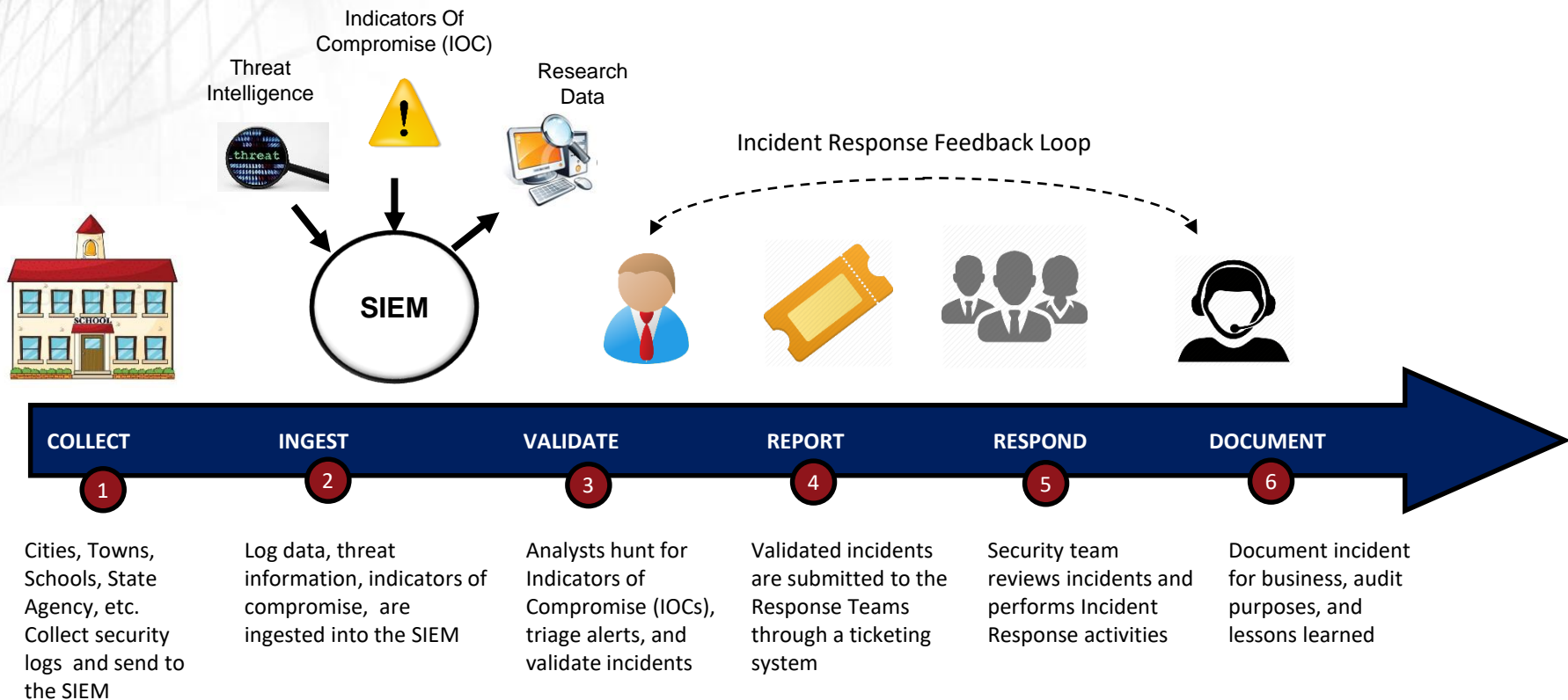
NCSF Advanced Certification Trainings

NCSF Engineering, Technical & Business Advanced Trainings

- The NCSF engineering, technical (operations) & business governance advanced trainings enable students to get hands on cybersecurity experience as part of a Security Operations Training Center (SOTC) model the university created to deliver NIST Cybersecurity assessment, testing and continuous monitoring services to businesses and governments not capable of doing it themselves. UMass can help training partners set up a SOTC of its own or provide SOTC services from its training SOC in Massachusetts.

  - **Location of Training:** Security Operations Training Center (SOTC) or Cyber Range
  - **Means of Instruction:** Classroom, Virtual Classroom & Self Paced Video
    Number of SOC/Range Hours: Varies per Program
  - **Prerequisites:** NCSF Foundation & Practitioner Certification
  - **Credentials Attained:** Digital Badges, PDU's, CEU's

NCSF Security Operations Training Center
Delivering SOC Services While Training the Workforce

Functions of a Security Operations Training Center (SOTC)

Indicators Of
Compromise (IOC)

Threat
Intelligence

Research
Data

Incident Response Feedback Loop

SIEM

COLLECT	INGEST	VALIDATE	REPORT	RESPOND	DOCUMENT
1	2	3	4	5	6
Cities, Towns, Schools, State Agency, etc. Collect security logs and send to the SIEM	Log data, threat information, indicators of compromise, are ingested into the SIEM	Analysts hunt for Indicators of Compromise (IOCs), triage alerts, and validate incidents	Validated incidents are submitted to the Response Teams through a ticketing system	Security team reviews incidents and performs Incident Response activities	Document incident for business, audit purposes, and lessons learned

NICE Certification Training

NCSF NICE Certification Training Library

- **The NCSF NICE Certification Training Library**, available via online video, prepares candidates to sit for the IT (CompTIA, Cisco etc.), information security (ISC², ISACA, CompTIA etc.) and Business Skill (Communication, Legal, Accounting etc.) certification exams aligned with the work and specialty roles outlined in the **NIST NICE Cybersecurity Workforce Framework (NCWF)**.

    - **Location of Training:** Online
    - **Means of Instruction:** Self Paced Video
    - **Number of Classroom Hours:** Varies per Program
    - **Prerequisites:** Varies Based on Certification
    - **Credentials Attained:** Certification, College Credits, PDU's, CEU's

NCSF Content Evaluation

- The NCSF Practitioner course digital book can be viewed at:

  URL: http://preview.skillpipe.com

  Then log in with:

  User: preview@skillpipe.com

  PW: courseware2017

- Chapter 8 of the NIST CSF Practitioner video course can be found at:
  - http://www.videotrainer.com/training/RunMobileCourse.aspx?CourseID=9082&CurriculumID=1601&demo=True

Questions & Answers