Signal Week
US Army NETCOM

SEI Overview

Brian D. Wisniewski

11 June 2012
**SEI Overview**

Presented at the CSM/SGM 2012 Mini-Conference June 2012 During the Network Enterprise Technology Command (NETCOM) CSM-SGM Conference, Ft Huachuca, AZ, 11 - 15 June 2012
Agenda

Introductions
  • Software Engineering Institute (SEI) Overview
Virtual Training Environment & XNET Overview
Scenario Introduction & Overview
Exercise Login and Orientation to the XNET Interface
Exercise Execution
Wrap-up and Conclusion
The SEI is a Federally Funded Research and Development Center (FFRDC).

Sponsored by the U.S. Department of Defense (DoD), it was created in 1984 and is administered by Carnegie Mellon University. It is a DoD R&D Laboratory.

Headquartered in Pittsburgh, Pennsylvania; the SEI provides support worldwide:

- 195 STE
- $150M annual revenue
- 600 employees
Mission and Strategy

Mission

The SEI provides technical leadership and innovation through research and development to advance the practice of software engineering and technology in support of DoD needs.

The SEI advances software engineering and related disciplines to ensure systems with predictable and improved quality, cost, and schedule.
SEI Objectives

The SEI works to:

- Identify, research, evaluate, and advise on software engineering technologies, trends, and practices.

- Collaborate with and leverage work found in industrial research, academia, and government laboratories.

- Mature promising software engineering technologies to enable standards, transition, and adoption within the DoD community.

- Enable government and industry organizations to make measured improvements in their software engineering practices.
A Broad Range of Stakeholders

The SEI advances research in software engineering and cyber technologies for its many stakeholders:

- Major government customers and sponsors
  - U.S. Department of Defense (DoD)
  - U.S. Department of Homeland Security (DHS)
- Researchers, developers, users, and acquirers—government, commercial, and academic
- Key industries and organizations with the potential to advance software engineering and related disciplines
- Strategic partners worldwide
SEI's Technical Strategy for Software-Reliant DoD Systems

- **Line-Funded Exploratory New Starts (LENS)**
  - Exploratory activities to identify risk/reward potential as a sustained research initiative (~1 year initial duration)
  - Sustained research initiatives (~3-4 year duration, depending on progress against measures of success reviewed annually)

- **Securing the Cyber Infrastructure**
- **Innovating Software for Competitive Advantage**
- **Advancing Disciplined Methods for Engineering Software**

Application of research to practice in acquisition programs & DoD/IC domains

EXPLORE  CREATE  APPLY  AMPLIFY  SUSTAIN
Key Capabilities & Core Competencies

The SEI researches & develops practices & methods in software engineering & related disciplines, applies them to real problems, & transitions them for broad impact.

The core competencies of the SEI are:

• **Process & Measurement**
  – Software development process and lifecycle (Planning, Requirements, Design, Coding, Testing, Verification, Validation, Sustainment/Support)
  – Cost estimation
  – Performance measurement
  – Producibility
  – Technical risk analysis & mitigation

• **Architecture**
  – Reengineering & reuse
  – Maintainability, changeability, & evolvability
  – Embedded software

• **Assurance & security**
  – Reliability
  – Security, safety, survivability, & timing
  – Cyber software assurance & forensics
Technical Program Alignment and Areas of Focus

- Securing the Cyber Infrastructure
- Innovating for Software Superiority
- Advancing Disciplined Methods for Software Engineering
- Accelerating Assured Software Delivery for the Mission

NSS: Networked Systems Survivability Program
RTSS: Research, Technology, & System Solutions
ASP: Acquisition Support Program
SEPM: Software Engineering Process Management Program
LENS: Line-funded Exploratory New Starts
Areas of Active Research and Development

- Models and Guidelines for Agility in DoD
- Acquisition Dynamics
- Static Analysis for Real-time Multi-Core
- Agile Architecting
- Edge Programming for Mobile Platforms
- Software Assurance Argumentation Theories
- Secure Coding Patterns for C, C++, and Java
- Malicious Code Detection and Analysis Techniques
- Trustworthy Embedded Systems
- Digital Investigations and Video Exploitation Gap Area Tools
- Socio-Adaptive Systems
- Probabilistic Modeling of Uncertainties in LCC
- Integrated, Lightweight, and Agile Life-Cycle Models
- Detection of Anomalies in DOD Data Repositories
# Customers & Stakeholders – Military Services

## Services

<table>
<thead>
<tr>
<th>Air Force</th>
<th>Army</th>
<th>Navy</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF/AQX</td>
<td>ASA/ALT (ASSIP)</td>
<td>DDG-1000</td>
</tr>
<tr>
<td>SAF/AQR</td>
<td>AMRDEC SED</td>
<td>EFV (Expeditionary Fighting Vehicle)</td>
</tr>
<tr>
<td>JMPS</td>
<td>Army Materiel Command</td>
<td>F/18</td>
</tr>
<tr>
<td>GEMS</td>
<td>ARDEC SED</td>
<td>F35</td>
</tr>
<tr>
<td>MMP Upgrade</td>
<td>CECOM SEC</td>
<td>PEO Integrated Warfare Systems</td>
</tr>
<tr>
<td>3DELRR</td>
<td>CERDEC C2C</td>
<td>PEO SUBS</td>
</tr>
<tr>
<td>C2AOS</td>
<td>HQDA G6/CIO</td>
<td>Submarine Warfare Federated Tactical System (SWFTS)</td>
</tr>
<tr>
<td>JMS</td>
<td>PdM NetOPS (PM WIN-T)</td>
<td>PMS 485</td>
</tr>
<tr>
<td>AF/A1 SOA</td>
<td>PdM Army Enterprise Systems Integration Program</td>
<td>(Maritime Domain Awareness)</td>
</tr>
<tr>
<td>DoD NextGen Chief Architect</td>
<td>PEO Aviation</td>
<td>SPAWAR Systems Center – Charleston</td>
</tr>
<tr>
<td>Support</td>
<td>PEO Soldier</td>
<td>NAVAIR</td>
</tr>
<tr>
<td>FAB-T</td>
<td>PM Battle Command</td>
<td>NAVOCEANO</td>
</tr>
<tr>
<td>PMAG and EELV study</td>
<td>PM FBCB2</td>
<td>Navy Cyber Defense Operations Command (NCDOC)</td>
</tr>
<tr>
<td>GPS III satellite and OCX</td>
<td>PM Heavy Brigade Combat Team</td>
<td>Communications Satellite (PMW 150)</td>
</tr>
<tr>
<td>N-CSDS</td>
<td>PM Integrated Air and Missile Battle Command System</td>
<td></td>
</tr>
<tr>
<td>Global Hawk GSRA and UCS ORS</td>
<td>PEO Integration</td>
<td></td>
</tr>
<tr>
<td>SAF/A6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AFRL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AFOSR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NASIC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The SEI is a Knowledge Pipeline: From Research to Transition

**EXPLORE**
- Cloudlets in Edge Computing
- Agile Architecting

**CREATE**
- ULS Systems Modeling
- Socio-Adaptive Systems
- Static Analysis for Real-time Multi-Core

**APPLY**
- System ATAM
- Integrated ACE/TSP
- Mission Thread Workshop
- Software Assurance Cases
- Architecture Competence

**AMPLIFY**
- SOA Certification Program
- V&B Documentation
- Operating Systems Analysis and Testing (OSATE)
- ATAM
- Software Architecture Curriculum
- QAW

**SUSTAIN**
- Maturity Models
- SMARRT Certification
- COTS Body of Knowledge
- SASS

**NSS**
- Threat Metrics
- Trustworthy Embedded Systems
- Secure Coding Standards
- Malware Analysis Tools
- Insider Threat Models & Controls

**RTSS**
- Malware & Forensics Analysis for Mobile Platforms
- Agile Architecting
- Cloudlets in Edge Computing
- SoS Architecture Patterns

**New R&D**
- Line-Funded Exploratory New Starts (LENS)
- Agility in DoD
- Acquisition Dynamics
- Acquisition Archetypes

**ASP**
- eLearning Pilots
- Technical Assessments
- Mission Success in Complex Environments
- Acquisition Strategy Workshop
Summary

25+ year history of contributions and innovation
World leader in software engineering research and transition
Strategic emphasis on enhanced impact
Current technical program spans acquisition, technical, and management practices
Positioned for future challenges
  • Extending current technologies
  • Exploring new technologies
Additional Briefings

Software Engineering Institute (SEI) Overview

CERT Cyber Threat & Vulnerability Analysis Overview

CERT Cyber Enterprise and Workforce Management Directorate Overview

Cyber Mission Assurance Overview
CERT Program

Mission
Anticipating and solving our nation’s cyber security challenges

Vision
A securely connected world

Strategy
Research, develop, transition, and support new security enhanced:
• software and system development technologies and practices
• system and network monitoring and management technologies and practices
• digital investigations and intelligence methods and tools
Anchor research and development efforts in operational challenges and realities
Pilot and prototype with strategic customers to set realistic transition paths

Goal
To reduce the opportunity for and impact of cyber attacks
Offensive cyber operations at the system, network, enterprise, critical infrastructure levels

Secure defensive operations at the system, network, enterprise, critical infrastructure levels

Security policies and plans

Workforce has the right knowledge, skills, abilities to conduct cyber missions and develop secure systems

Art and science of building securable technology

Understand the tactics, techniques, and procedures (TTPs) of the community and adversary

Offensive Operations

Defensive Operations and Security Management

Policies and Plans

Workforce Development

Secure Software and Systems Engineering

Cyber Intelligence

Software Engineering Institute

Carnegie Mellon
Research Challenge in Cyber Security

Threats at Scale in number and time

- Adversaries can affect millions of connected objects in very compressed time frames
- Immense attack surfaces: computers, applications, services, networks, routers, users, physical control connections, databases, business operations, etc.
- Sub-second timescales for attacks, responses, situational awareness

We don’t know yet how to effectively deter, prevent, detect, respond in a way to mitigate important threats at scale.

- How to acquire, design, build, compose, and operate software components and systems to support the survivability of the mission.
- How do we ensure that future generations of technology will better protect our critical systems and not inhibit innovation, agility, resiliency?
- We’re making progress, but the gap is a national security issue

CERT’s research approach

- Exploit data collected to mitigate threats and attacks.
- Exploit data collected to inform development of secure/resilient software, systems, networks, services, etc.
- Develop scalable cyber-security forensics
- Share data and experiences
## CERT Program Organization

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Software and Systems</td>
<td>Develop technologies to embed software and system assurance in all aspects of the system development life cycle.</td>
</tr>
<tr>
<td>Cyber Enterprise &amp; Workforce Development</td>
<td>Establish the routine use of disciplined approaches to improve enterprise survivability and resiliency; provide security practices and information assurance training and education.</td>
</tr>
<tr>
<td>Cyber Threat and Vulnerability Analysis</td>
<td>Discover and resolve vulnerabilities in software products; improve cyber-tradecraft analysis; quantitatively assess potential threat and subsequent impact of malicious activity.</td>
</tr>
<tr>
<td>Digital Investigations and Intelligence</td>
<td>Research and Develop gap area technologies to advance the state of practice of digital exploitation and analysis.</td>
</tr>
</tbody>
</table>
Secure Software and Systems

Develop and adapt practices, processes, tools, techniques, and measures to address security and survivability in every phase of the development and acquisition life cycle

Motivation:

- Threats to DoD systems evolving
- Potential for crippling attacks
- Dependence on large-scale, complex, software dependent systems
- Early decisions in Acquisition & Development have major impact on security

Primary areas of work:

- Address security across the software engineering life-cycle to improve security properties
- Software and System development technologies and practices
- Embedded system safety, security, and survivability
Secure Software and Systems Organization

Cyber Security Engineering
- Acquisition and Development Practices
- Software Assurance Education
- Supply Chain Risk
- Security Measurement and Metrics

Secure Code Initiative
- Code Construction
- International Standards
- Code Analysis
- Analytical Tools, Methods, and Practice

Next Generation Security Mechanisms
- Trustworthy Embedded Systems
- Survivable Infrastructure

Software Engineering Institute
Carnegie Mellon
Digital Intelligence and Investigations

*The Digital Intelligence and Investigation Directorate continuously searches the horizon for the digital investigative challenges of tomorrow. Our position at the nexus of law enforcement, intelligence, industry, and research allows us to maintain a forward perspective on the potential challenges of the future.*

- We administer direct operational support to key customers, and focus our applied research capabilities to solving critical gap areas problems and limitations.

- We provide highly specialized computer forensics and incident response “gap area tools” not addressed by commercial tools or standard techniques to the DOD and US Federal Civilian Law Enforcement Agencies.

**Advantage**

- Consistent identification of emerging challenges
- Access to data otherwise impossible
- USG gains access to rapidly prototyped capabilities
- Clear understanding of limitations with: commercial technology; training gaps; and techniques.
- Amplified transition directly to operational units combating adversaries
Notices

© 2012 Carnegie Mellon University
This material is based upon work supported by the U.S. Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY
THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.
Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT ® is a registered mark owned by Carnegie Mellon University.
CERT™ Cyber Threat and Vulnerability Analysis
CERT Program

Carnegie Mellon

Software Engineering Institute

Acquisition Support

Research Technology and Systems Solutions

Software Engineering Process

Cyber Enterprise and Workforce Management

Digital Investigations and Intelligence

Cyber Threat and Vulnerability Analysis

Secure Software and Systems
Cyber Threat and Vulnerability Analysis

Perform, improve and grow capacity in:

- “Tier-3” analysis for USG cyber operations
- Test, evaluation, review and workflow of cyber-security-enabling technologies for USG operations and program offices
- Cyber operations in Critical Infrastructure and Key Resources (CIKR)
CTVA Functional Breakdown

Cyber Threat and Vulnerability Analysis

Operational Analysis
Applied Innovation
Best Practices
Capacity Building

DOD & Intel
Federal & LEO
Code Analysis Techniques
Network Analysis Techniques
Trends
Analysis TTPs and Design Guidance
Mentoring & Workshop
Reference Data and Tools
DOD CND Architecture

DOD CND Architecture OV-1, NSA, June 2010
Areas of Work

Malicious code analysis

Critical infrastructure incident analysis

Network situational awareness

Software vulnerability analysis
Malicious Code

<table>
<thead>
<tr>
<th>Mission</th>
<th>Focus Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop new malicious code analysis insights, technologies, practices, and capabilities, to better counter and exploit adversarial use of information and communication technologies.</td>
<td>• Static analysis (reverse engineering)</td>
</tr>
<tr>
<td>• Defence Community</td>
<td>• Run-time analysis</td>
</tr>
<tr>
<td>• Intelligence Community</td>
<td>• Code comparison and characterization</td>
</tr>
<tr>
<td>• Federal Law Enforcement Community</td>
<td>• Large-scale collection</td>
</tr>
<tr>
<td>• Homeland Security / Federal Agencies</td>
<td>• Capacity building</td>
</tr>
<tr>
<td>• Federal Researchers</td>
<td></td>
</tr>
</tbody>
</table>
Malicious Code CONOP

Stakeholders
- Incident responders
- LE and CI investigators
- Network and security operations
- Intel and all source analysts

Malware
From
- Forensics investigation of an incident
- Intelligence

submitted for analysis

Triage
- Hashing
- Classification & Similarity
- Binary Unpacking
- Run-time Analysis

produces

indicators
- trends, targeted analysis, situational awareness, and insights

Analysis
- Reverse engineering
- Fusion

produces

Malware
Catalog
- original binary, unpacked, drop-files
- Derived Data
  - Touch points: network and host
  - Hash: file, section, and function
  - Classification: entry point and AV
  - Code analysis results
  - Linkages and relationships

archive malware and meta-data

Automation Insights

archive analysis results and supporting artifacts

Software Engineering Institute  Carnegie Mellon
## Incident Analysis in the CIKR

<table>
<thead>
<tr>
<th>Mission</th>
<th>Focus Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assisting USG and industry in combating advanced persistent threat</td>
<td>• Incident analysis</td>
</tr>
<tr>
<td>• USG sector-specific leads</td>
<td>• Exercises</td>
</tr>
<tr>
<td>• Information Sharing and Analysis Centers (ISACs)</td>
<td>• Capacity building</td>
</tr>
<tr>
<td>• CSIRTs with National Responsibility</td>
<td></td>
</tr>
</tbody>
</table>
CIKR Collaborative Operations CONOP

Private-Sector Company

- Protect
  - Controls and risk profile
  - Lesson Learned, Indications, and Warning
- Detect
  - Incident
  - Security Operations Center (SOC)
- Respond
  - Incident response and recovery

Broader Community

- Product CSIRTs
  - Share
- National CSIRTs
  - Operational relationships
  - Coordinates & Supports

Recording

Protect and risk profile

Detect

Respond

Informs

Enforce

Monitoring finds

Initiates

Support

Share

Operational relationships

Support

Informs

Share

Operational relationships

Support

Operational relationships

Support

Software Engineering Institute

Carnegie Mellon
# Network Situational Awareness (NetSA)

<table>
<thead>
<tr>
<th>Mission</th>
<th>Focus Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantitatively measure baselines, vulnerability, threat, and intrusions to infrastructure from the network perspective</td>
<td>• Sensor development</td>
</tr>
<tr>
<td>• Pervasive USG CND monitoring efforts</td>
<td>• Network analytics</td>
</tr>
<tr>
<td>• Discovery missions</td>
<td>– Topology mapping</td>
</tr>
<tr>
<td>• Survey missions</td>
<td>– Traffic analysis</td>
</tr>
<tr>
<td>• Enterprise policy makers and system architects</td>
<td>– Situational awareness</td>
</tr>
<tr>
<td></td>
<td>• Network test-beds</td>
</tr>
<tr>
<td></td>
<td>• Standards</td>
</tr>
<tr>
<td></td>
<td>• Metrics</td>
</tr>
<tr>
<td></td>
<td>• Capacity building</td>
</tr>
</tbody>
</table>
NetSA Historical Focus Areas


Operational Data Analysis

AirCERT .gov networks NIPRNet and SIPRNet Coalition Networks National Incidents

Analytics

Scan Detection Mission Use Assessment Close Network Defense Sensor Efficacy/Placement metrics

Topology Mapping → Rogue Server Detection

Uncleanliness Vector “Spike” Detection Network Touch Points

“Working Set” analysis Beacon Detection “Generated DNS name” detection

Routing Backdoor Detection Hilbert curves → existence plots → Spark lines

Behavioral Flow Signatures

Sensors

Intrusion Detection Flow Metadata Active Defense

Flow

Intrusion Detection

Standards

IETF IDMEF IETF Information Flow Export (IPFIX)

IETF Incident Object Description Exchange Format (IODEF) National Information Exchange Model (NIEM)
## Vulnerability Analysis

<table>
<thead>
<tr>
<th>Mission</th>
<th>Focus Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reducing the birth rate and increasing the death rate of software vulnerabilities;</td>
<td>• Vulnerability remediation</td>
</tr>
<tr>
<td></td>
<td>• Secure configurations</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability management</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability discovery</td>
</tr>
<tr>
<td>• USG watch-and-warning centers</td>
<td></td>
</tr>
<tr>
<td>• CNA/E mission owners</td>
<td></td>
</tr>
<tr>
<td>• Vulnerability researchers</td>
<td></td>
</tr>
<tr>
<td>• Software vendors</td>
<td></td>
</tr>
</tbody>
</table>
Software Vulnerability CONOP

- **Discovery**: Finding new vulnerabilities in existing software
- **Analysis**: Gain understanding of new vulnerabilities
- **Coordination**: Working with vendors and researchers to respond to vulnerabilities
- **Disclosure**: Providing vulnerability info to the public
- **Remediation**: Applying fixes and workarounds for deployed vulnerabilities
- **Mitigation**: Systemic and environmental changes to reduce the risks posed by vulnerabilities

- **Exploit**: Make a reliable, working exploit
- **Adapt**: Make exploit available for technical targeting
- **Field**: Use for an operation
CERT Cyber Enterprise and Workforce Management Directorate
Cyber Enterprise and Workforce Management

Cyber

Describes the boundary of our work: assets that are bound together by networks

Enterprise and Workforce

Describes the entities on which our work is primarily focused

Management

Describes the type of cyber security activities on which we primarily concentrate

CEWM’s work engages all three critical dimensions for effectvely managing cyber security.
CERT CEWM Overview
What is CERT®-RMM?

CERT-RMM is a maturity model for managing and improving operational resilience.

“...an extensive super-set of the things an organization could do to be more resilient.”
- CERT-RMM adopter

- Guides implementation and management of operational resilience activities
- Converges key operational risk management activities: security, BC/DR, and IT operations
- Defines maturity through capability levels (*like CMMI*)
- Enables measurement
- Improves confidence in how an organization responds in times of operational stress
### CERT-RMM: 26 process areas

#### Engineering
<table>
<thead>
<tr>
<th>ADM</th>
<th>Asset Definition and Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL</td>
<td>Controls Management</td>
</tr>
<tr>
<td>RRD</td>
<td>Resilience Requirements Development</td>
</tr>
<tr>
<td>RRM</td>
<td>Resilience Requirements Management</td>
</tr>
<tr>
<td>RTSE</td>
<td>Resilient Technical Solution Engineering</td>
</tr>
<tr>
<td>SC</td>
<td>Service Continuity</td>
</tr>
</tbody>
</table>

#### Enterprise Management
<table>
<thead>
<tr>
<th>COMM</th>
<th>Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP</td>
<td>Compliance</td>
</tr>
<tr>
<td>EF</td>
<td>Enterprise Focus</td>
</tr>
<tr>
<td>FRM</td>
<td>Financial Resource Management</td>
</tr>
<tr>
<td>HRM</td>
<td>Human Resource Management</td>
</tr>
<tr>
<td>OTA</td>
<td>Organizational Training &amp; Awareness</td>
</tr>
<tr>
<td>RISK</td>
<td>Risk Management</td>
</tr>
</tbody>
</table>

#### Operations Management
<table>
<thead>
<tr>
<th>AM</th>
<th>Access Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>Environmental Control</td>
</tr>
<tr>
<td>EXD</td>
<td>External Dependencies Management</td>
</tr>
<tr>
<td>ID</td>
<td>Identity Management</td>
</tr>
<tr>
<td>IMC</td>
<td>Incident Management &amp; Control</td>
</tr>
<tr>
<td>KIM</td>
<td>Knowledge &amp; Information Management</td>
</tr>
<tr>
<td>PM</td>
<td>People Management</td>
</tr>
<tr>
<td>TM</td>
<td>Technology Management</td>
</tr>
<tr>
<td>VAR</td>
<td>Vulnerability Analysis &amp; Resolution</td>
</tr>
</tbody>
</table>

#### Process Management
<table>
<thead>
<tr>
<th>MA</th>
<th>Measurement and Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>MON</td>
<td>Monitoring</td>
</tr>
<tr>
<td>OPD</td>
<td>Organizational Process Definition</td>
</tr>
<tr>
<td>OPF</td>
<td>Organizational Process Focus</td>
</tr>
</tbody>
</table>
Development and Operational Guidance End-to-End

Plan -> Design -> Develop -> Acquire -> Deploy

CMMI-DEV (software development)

CMMI-ACQ (software acquisition)

CERT-RMM (secure, continuous operation)

CMMI-SVC (service quality)

TSP (data-driven quality approach for team management, applicable to projects throughout lifecycle)

DEVELOPMENT

OPERATION
CERT Insider Threat Center

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Our mission: The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.
CERT Insider Threat Center Objective

Opportunities for prevention, detection, and response for an insider attack

INSIDER

HR, Legal, Physical Non-tech indicators
Prevent
Detect
Respond

Timeline
Tech indicators

Software Engineering Institute | Carnegie Mellon
Insider threat research develops this…
Deriving Candidate Controls and Indicators -2

And turns it into this…

Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *" | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab" sender_address | fields -Account_Name] total_bytes > 50000 AND recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address, recipient_address, message_subject, total_bytes'
DoD Cyber Workforce Development

Challenges

- Inability to “train as you fight” as part of routine operations
- Inability to accurately assess mission readiness of cyber units/crews
- Lack of real-time modeling and simulation tools for lifelike skills practice and assessment

SEI Response

- CWD Capabilities Definition and Measurement
- CERT Exercise Network (XNET)
CERT XNET

Goals of XNET:
• Convenient and Efficient Access to Range AND Scenarios
• Robust individual/team evaluation
• Advances in Mod/SIM
• Operationalize DoD Cyber Community

DoD Utilization:
• USCYBERCOM Cyber Flag exercises
• Army Reserve Information Operations Command pre-deployment evaluation
• OSD/NII International Cyber Defense Workshop (ICDW)
• Army Theater Cyber Center of the Year competition
Cyber Flag

USCYBERCOM sponsored, world-class cyber exercise
Exercise Service Components and JCCC in tactical cyber operations;
progressive complexity over 4 mission days

12-1 Advances:
- Xcloud 1.0; 4,000 dynamically provisioned, controlled hosts/devices; 1-click roll-back, integrated record/playback
- Embedded Cyber Situational Awareness and COP 1.0
- “Whack a Mole” OPFOR
- 2,700 simulated users with under-the-floor, real-time control

13-1 Development:
- Automated helpdesk for “complaining users”
- COP 2.0; synergized feeds
- Kinetic CND (based-on Scadaville)
- Xcloud 2.0; instrumented for real-time lessons learned, BDA
Notices

© 2012 Carnegie Mellon University

This material is based upon work supported by the U.S. Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® is a registered mark owned by Carnegie Mellon University.
Cyber Mission Assurance (OSD CAPE)
Overview

Quick overview of “research vision” for the Cyber Mission Assurance work

Client example: Leveraging Cyber Mission Analysis Method(s) in support of OSD CAPE goals and objectives

Questions?
Cyber Mission Analysis Research Focus

Challenges

- Lack of understanding of network and mission impacts when capabilities are reduced
- Facing continually evolving adversary tactics, techniques and procedures (TTPs) to gather information and disrupt network/mission operations
- Very limited opportunities and resources to “train as you fight”

Research Approach & Innovations

- Leverage SoS architecture-centric methods with NSS’s cyber security initiatives to create a catalog of mission thread artifacts which can be used to analyze DoD networks for mission assurance and architectural agility and resilience
- Automation Framework to generate attacks which is integrated with XNET to perform cyber security workforce development and training based on the mission thread artifacts

Impact to DoD

- A streamlined and repeatable mission analysis method to improve mission assurance and situational awareness for cyber warriors and the missions being executed
- A single technique that enables the mission needs to drive architecture and training
Mission Assurance Research: Guiding Scenario

An adversary is interested in gaining footholds into DoD networks via its computer network exploitation methods.

Two key points of interest have been identified:

- Naval Personnel Information at Port Hueneme
- Naval Maintenance Operations – San Diego
Guiding Scenario – Current Approach

1. Adversary performs “phishing” attacks and compromises 3 workstations in each network and a privileged account on the Personnel system.
2. US imposes tariffs and sanctions on adversary country; Intelligence reports note adversary is considering taking some action.
3. Adversary starts Denial of Service Attacks on Operations system.
4. Users start to complain about slow operation of their system.
5. Adversary begins exfiltration of personnel information.
6. Adversary stops attack after personnel information is downloaded.
7. Adversary stops DOS attacks.
8. Network admins notice DOS attack has stopped and begin network battle damage assessment.
9. Network admins notice data has been exfiltrated two days after incident; Investigation is started.

Software Engineering Institute | Carnegie Mellon
Guiding Scenario – Desired End State

1. Navy locations identify key missions and cyber dependencies to drive training using the latest automated technologies

2. Adversary performs “phishing” attacks and compromised 3 workstations in each network and a privileged account on personnel system

3. Adversary starts Denial of Service Attacks on Operations system.

4. Users notice slow operation but critical functions continue

5. Network admins detect a possible threat pattern

6. Adversary begins exfiltration of personnel information.

7. Network admins confirm threat pattern and mission impact

8. Network admins stop attack shortly after download is attempted

9. Adversary stops DOS attacks

10. Network admins assess variations in attack patterns and mission areas being targeted to update and conduct training

Adversary’s System

Operations System

Personnel System
Properties of Desired End State

Clear Mapping to Cyber S&T Priorities*

- **Increasing Adversary / Defender relative work:** The cyber attack is stopped with fewer resources on the part of the defender
- **Assuring Effective Missions:** The critical missions were identified and related to cyber vulnerability and attack patterns to enable rapid detection and reaction to the attack.
- **Resilient Infrastructure:** The critical system functions were identified and mapped to architectural dependencies to build-in mission assurance

Assertions to Achieve Cyber S&T Priorities

- Long term automation objective requires understanding the analytical framework, technical dependencies and patterns of cyber operations
- Enabling rapid, repeatable and flexible training is critical both in the near term and to utilize eventual automation techniques

*Cyber S&T Priority Steering Council Research Roadmap, NDIA Disruptive Technologies Conference, 8 Nov 2011*
**Task A1: Create a catalog of cyber security mission thread artifacts**

**Problem 1**

Can an approach be developed to enable our cyber warriors to quickly gain an understanding of operational impacts on their networks and missions when cyber actions are considered in response to attacks/threats?

- Need an approach which can be used to analyze and evaluate the agility and resilience of the infrastructure
- The approach must support mission assurance analysis
- The approach needs to be able to address changing adversary TTPs
- Risk identification and prioritization is a key aspect that must be addressed

- Develop OV-1s, Vignettes, End-to-End Mission Threads
- Mission Thread Workshop
- Mission Thread Workshop
- Mission Thread Workshop
- Augmented End-to-End Mission Threads
- Application of External R&D Efforts
- CONOPS
- Fed into DoD Architectural Process (OV-2, OV-5, OV-4, OV-6c)
- SoS-level Use Cases (functional threads)
- System Quality Requirements
- Architectural Challenges
- Development of Cyber Security Architectural Patterns Catalog
- Development of Cyber Security Mission Threads Catalog
- Key
  - DoD 5000 Acquisition Documents
  - Program’s Tailored Byproducts
  - SEI Research Products
  - Key Benefits
  - SEI methods

Key

Software Engineering Institute
Task A2: Develop Cyber Security Workforce Development Framework

Solution

1. Work with the XNET team to incorporate the use of the mission thread artifacts to create a catalog of scenarios
2. Work with the Malicious Code team to define requirements and develop a malware-like framework which supports XNET and the scenarios being developed
3. Based on previous XNET cyber exercises, evaluate traffic/data generation capabilities and the need to enhance the XNET capabilities to support the scenarios being developed
   • internal application, MIT’s Lariat or other external applications
   • external interfaces to real/simulated hardware/communication links
4. Pilot with organizations with existing XNET setups
Task A2: Cyber Security Workforce Development Training Approach
Supporting client need: OSD CAPE

Mission

OSD CAPE responsibilities include:
• analyzing and evaluating plans, programs, and budgets in relation to defense objectives and threats
• providing leadership in developing improved analytical tools for analyzing national security planning
• ensuring that the costs of DoD programs are presented accurately and completely

SEI Objective

Enable DOD to develop a Cyber Front End Assessment Model and Approach that:
• prioritizes OSD C4 mission objectives
• develops executable mission threads in order to create high impact and realistic scenarios that drive unit, component and joint virtual training exercises (and modeling and simulation)
• results in data collection and metrics that can be leveraged to make meaningful IT/Cyber programmatic decisions

Challenges with current approach
• Treating each exercise as a “one-off” event is inefficient and doesn’t support consistent measures for analysis across events
• Lack of clarity around defined resiliency measures
• Need for objective ways to measure and analyze exercise results

Adapted from http://www.cape.osd.mil
OSD CAPE: Approach

Leverage multiple SEI methods:

- Apply RTSS Architecture-Centric Mission Thread method to prepare for upcoming cyber exercise scenarios
- Work with CERT Network Situational group to bring into consideration real-life issues they are addressing supporting DoD networks
- Apply CERT Resilience Management Model as the framework to define resiliency measures

Work with CERT Malicious Code group to get an understanding of how an attack (like phishing or a PDF-exploit) works and incorporate that into the mission thread

Participate in exercises to analyze effectiveness of cyber mission threads and collect resiliency measurement data for post-event analytics

Revise baseline mission threads and measures that can be leveraged for next exercise
OSD CAPE: End-to-End Lifecycle

- Mission Objectives
  - Create daily scenarios for the exercise
  - DoDAR-like views (OV-1, -3 and -4)
  - Vignettes
  - Mission Threads
  - Quality Attributes
  - Risk Drivers

- Mission Threads Artifacts
  - Worked with CYBERCOM and OSD CAPE to revise artifacts
  - Applied NSS’s cyber security initiatives methods in the areas of Resilience Management Model and Network Situational Awareness

- Data Analysis
  - Cyber exercise based around XNET

- Events
  - Architecture evaluations
  - Risk identification

Identify
- Cyber security architectural patterns
- Mission area needs
- Tactics, techniques and procedures
- Training needs

Identify exercise lessons learned

KEY
- Green – occurred
- Yellow - envisioned

Software Engineering Institute | Carnegie Mellon
Impact

- SEI preliminary mission threads were used during the cyber exercise pre-planning meeting, led by LCDR Michael C. Holland USCYBERCOM J-73, to develop scenarios for the December Cyber Flag exercise.

- Information provided by the SEI, and others, is being used at the initial planning conference for this year’s cyber exercise mission to help prepare for the next exercise.
  
  - For example, mission threads providing additional detail about threats origination are likely to be used to decide where to put sensors for the next exercise.

Impact Statement Dr. Dixon, OSD CAPE (paraphrased):

“Cyber Flag daily scenarios were significantly enhanced due to the mission thread method.”
Recent OSD CAPE Activity (2/28/12)

Completed delivery of data analysis efforts from Cyber Flag 12-1

- Identified what information was able to be recorded during the exercise (through sensors), as well as what information was not able to be captured due to sensor placement, storage, etc.
- Identified what additional information could be obtained in future cyber exercises based on:
  - Earlier and more detailed pre-planning for the cyber exercise
  - If additional resources were applied to existing setup
- Provided proposal to OSD CAPE client for how to apply the end-to-end cyber mission assurance approach (circle flowchart graphic)

Other potential and current clients applying approach

- Currently leveraging secure mission thread approach on DHS S&T Commercial Warning Automated System (CMAS) project
  - Mission threads used to define emergency response scenario analysis and to identify security threat risks
- OPNAV N-81 interested cyber defense and modeling
- Multiple related discussions across DoD and Intel community
- Developing research proposal targeted at establishing a Mission Assurance program initiative
OSD CAPE Next Steps

Data Planning/management/processing for a cyber exercise

• Requested SEI’s continued support for Cyber Flag 13-1 planning and exercise data observer
  – Provide a new work plan which reflects guidance and options provided
• Continue to focus on improving the ability to record and analyze data
  – Based on vignettes/scenarios being proposed to CYBERCOM for Cyber Flag 13-1:
    • Identify how best to take advantage of existing equipment
    • Identify possible additional data collection capabilities and associated costs
  – Consider providing remote data analysis capabilities for the exercise

Data processing/analysis for cyber mission assurance

• Augment the vignettes/scenarios based on mission assurance approach to identify possible options within the scenarios and the ability to record the information to confirm the events which occurred
• Work on developing the vignettes/scenarios to better reflect current operational situations
• The augmented vignettes/scenarios will be offered by OSD CAPE to CYBERCOM for consideration in Cyber Flag 13-1
How is this related to today’s Challenges?

“We have an independent strategic assessment group made up of senior experts from a whole variety of disciplines across military and civilian organizations … So the recommendations really took on and I think I’m excited about a lot of these… We’ve got to analyze what are the things that are most important to us, prioritize them and decide how do we defend them. We’ve got to establish machine-to-machine situational awareness relationships, both in and out of the defense focused networks. Create and incorporate automated indications and warning that are smarter than we are. They know when an attack might be occurring and can warn us ahead of time instead of telling us that something has occurred. Create the ability to characterize better. Look for the cause, the risk and the mitigation of an event.

Interesting comment out of this [assessment] group that people need to be reminded that the networks aren’t the mission, the networks support the mission, and I think there was a period of time where we maybe kind of strayed a little bit and looked at cyber as its own art form and it was the mission and, in fact, like space it enables all of those missions to occur and if we’re not looking at it from that broad enterprise aspect we will probably not be successful.”

10.20.09 - REMARKS BY GENERAL GENE RENUART at the AFCEA Defending America, Cyber 2010
Questions?
Virtual Training Environment (VTE) and XNET Overview
NETCOM - VTE & XNET

Overview of VTE
Overview of XNET
Integrating VTE & XNET into NETCOM Training
VTE  (http://vte.cert.org)

Asynchronous Knowledge and Skill building

• Captured Classroom Lectures
  – Slides, Video, Transcript, Learning Management System
  – Enterprise management tools
• Instructor Demonstrations
  – Narrated Screen-recordings that teach specific skills
• Hands-on Labs
  – Practice for developing cybersecurity skills
VTE  (http://vte.cert.org)

Entry Level Training

- Security +
- IAT Level I
- IAM Level I

Advanced Level Training

- CISSP
- CISA
- ISSEP

Technology Specific Training

- IPv6
- Wireless Security
- SiLK & Netflow Analysis
The Cyber Exercise Challenge

How to make cyber exercises routine, realistic, repeatable, and cost effective?

• Logistics
  – Travel and facility cost
  – Building/managing exercise infrastructure

• Complexity
  – Difficult to create realistic and current scenarios
  – Exercise infrastructures too monolithic

• Outcome
  – Limited benefit to workforce cyber readiness
Solution: CERT Exercise Network (XNET)

Browser-based access to mission-specific cyber-exercise environment

Frees units from the resource intensive tasks of…

• building
• deploying
• administering

...the exercise environment

Allows controllers to focus on exercise objectives
XNET Overview

Web-based Access
Centrally managed Infrastructure
Customizable Scenarios
Structured Control
Team Collaboration
Assessment and Observations
Access

Requires

- Web Browser, Java, and Internet connectivity

Self-contained environment

- Scenario network traffic contained in virtual sandbox via RDP Air-Gap

Geographically Separated Teams have Instant Access to Live Exercise Scenarios
Centrally Managed Infrastructure

NextGen Virtualization
Granular Exercise control
Can “Plug-In” to DoD Ranges
Customizable Scenarios

XNET allows you to:

- Create your environment
- Create your events
- Create your timeline
Customizable Scenarios – Forensics

XNET utilized to provide a real-time Forensics Challenge for Annual Cyber Defense Exercise

Access to CERT Forensics Appliance, LiveView Images, C-CAP

Notional Captured Workstation – Native Arabic XP Install
Structured Control

On-the-Fly modification
• Timeline and Event Library

Realistic Threats
• Drag and Drop attacks/anomalies
• Robust traffic generation

Automated data collection
• Real-time readiness metrics
Team Collaboration

Chat
• Instant out-of-band communications

White boards via WIKI pages
• Collaborate on problems, share ideas, answer team questionnaires

Scenario Maps
• Share remote desktop (learn from others)
• Work as a team in a single environment
Assessment and Observation

Allows users to:
• Provide Feedback
• Take Quizzes
• Submit Reports

Allows evaluator to:
• Glean Instant feedback
• Pose Leading Questions
• Evaluate users responses
• Access Automated Scoreboard
XNET: Force Utilization Examples

US Army NETCOM
USAF
US Army Reserves
OSD/NII
NSA
DHS / US-CERT

Scene 1
09:30
Scene 2
Scene 3
Scene 4
09:45
STARTEX
09:45
Chaff
10:00
Phishing Email
10:05
Hosts Compromised
10:20
Phishing Email Reported
10:25
Data Exfiltration
10:45
Bot-net Downloaded
10:55
Bot-net Spreads
Infrastructure

Fixed (Primary)
Deployed
(secondary alternative - limited capabilities)
OPERATION ELITE MERCURY
“Gaining Cyber Dominance”

U.S. Army NETCOM

Cyber Centers’ Computer Network Operations (CNO) and Computer Network Defense (CND) teams

Initial Individual Training (VTE)

Collective Monthly Exercises

Annual Capstone Exercise / Assessment – “Best Cyber Center” Award
XNET Scenario Introduction

Brent Kennedy

27 March 2012
Example Scenario Overview

Our scenario today was utilized during mission validation of the U.S. Army Reserve Information Operations Command’s Detachment 52 in its preparations for mobilization and deployment to Cyber Center SWA.

Your mission is to gain full situational awareness of the network including normal and abnormal traffic.

The exercise is divided into 2 overall sections.

The first section will be network reconnaissance which includes familiarization with the systems and tools, benchmarking the network traffic, and testing all hosts for vulnerabilities.

The second section will introduce active attacks. As a collective group, you must identify the attacks to determine what they are doing and where they are coming from.
Scenario Overview (continued)

The network you must protect is divided into 3 parts: NOSC, Fort Hood, and Fort Huachuca.

The NOSC is "physically" located at Fort Hood but can be thought of as a separate network.

During your network reconnaissance take a close look at each network. You should have a full understanding of all the hosts they contain as well of the traffic coming in, out, and within.
Scenario Overview (continued)

Topology overview

External scanning
Zones: NOSC, Hood, Huachuca
Actions: Login to Arcsight from Mgmt machines
What to look for: port scan notifications
Highlights: Arcsight
Exercise Environment
Exercise Environment (continued)
Exercise Environment (continued)
Exercise Environment (continued)
Scenario Overview (continued)

User scanning
Zones: Hood, Huachuca
Actions: Use retina on Mgmt machine to scan user subnet
WTLF: # hosts unpatched (IPs:…)
Highlights: Retina, Nessus
Scenario Overview (continued)

SQL Injection  
Zones: Hood  
Actions: Have Arcsight Open from Mgmt machines  
WTLF:  
‘SQL Injection’ and ‘TFTP’ log entries  
Web logs with attack string  
Highlights: Arcsight
Scenario Overview (continued)

Data Exfiltration
Zones: Huachuca
Actions: Open wireshark on internal and external snort
WTLF: data packets from 3 exfiltrations; all 3 send ‘Sherlock Holmes’ over the wire
Highlights: Wireshark
Scenario Overview (continued)

Create HBSS ePo report (time permitting)
Zones: NOSC, Hood, Huachuca
Actions: Connect to ePo server and generate report on users
WTLF: ePo interface and report
Highlights: HBSS ePo
Exercise Login

1. Please open Internet Explorer and navigate to http://xnet.cert.org
2. Please click on the green LOGIN button in the upper right hand corner.
3. Please login using the credentials on your name placard in front of you.
4. Your screen should now appear similar to the one at the right.
5. Please click on the “Connect” button under IE Access.
6. You may be prompted about allowing the RDP client to access the website and about accepting the self-signed certificate. Please click on “Connect” and “Yes” respectively.
7. Once you are logged in, please give one of our instructors a thumbs up.
Welcome to XNET

As present, you are at the Mission tab. Click here to access the scenario specific information.

To access the scenario topology, click on the Map tab. Once you are on the Map tab, you will see the Afghan Mission Network. Each circle on this map represents a unit supporting operations in the Afghanistan theatre. Your team will be representing “AFIT Al Udeid AFB, Doha, Qatar”. Click on the circle named AFIT1 to view the NGO’s network that was compromised and access the CERT’s Clustered-Computing Analysis Platform (C-CAP). Double click a machine on the C-CAP portal to view the console for that system.

Click on the Systems page holds multiple machines open in tabs.

Quizzes are used to test your understanding of the scenario. These are available under the Eval tab. These evaluations will guide you through the tasks that you need to accomplish for this scenario. Please keep in mind that only one person on a team can edit a quiz at a time.

Once the challenge is over, the final results will be published under the Score tab.

There are a couple of forensics labs available under the Labs tab. These labs are useful resources on forensic collection and analysis of volatile and persistent data.

Manuals of these labs are available on the exercise page. To start a lab, click the green button. This will deploy virtual machines for that lab. Follow the instructions in the lab manual to carry out the lab. Once done, hit the red button.

Team coordination features

Tab is useful for sharing notes and important information amongst the team members.

Chat windows on the bottom left lets you chat with other participants. From the dropdown menu, you can select either a team name to send message to the entire team or a team member to chat privately.

Tab is used to record participants activity in XNET. To start recording, click the red button. Stop the recording using the same button. To play the video, right click on the clip and select play.

Use the button to logout of the portal.
Scenario Overview

Stage 1:
Normal chaff
  • User internet traffic
  • Local domain traffic
  • Typical external port scanning (e.g., port 22, 80, etc.)
Vulnerability analysis
  • Network situational awareness (benchmark)

Stage 2:
Increased external probing
  • DoS
Sensor familiarization
Illegal software installed

Stage 3:
Intrusion detection
  • SQL injection
  • IRC chat

Stage 4:
Intrusion detection:
  • Insider threat
    • DoS
    • Data exfiltration
      • Easy/medium/hard
Malicious PDF released (malware)
  • Detection of malicious file, processes, etc.

Stage 5:
Threat analysis of malware
Debrief
Scenario Execution

“Weapons Free”
Scenario Wrap Up – Review Stage 1

CDAP:
• Analyze 4 servers, 20 users
• Identify 1 host w/o SP
• Identify 1 server missing a patch
• Identify 1 server running anonymous FTP

CND:
• Establish baseline w/Arcsight, Snort
• Find open ports of concern on firewall (23, 37331, etc.)

IH:
• Run Retina scans (Findings?)
Scenario Wrap Up – Review Stage 2

CDAP:
• Find unauthorized software installations
• 2 occurrences on different hosts

CND:
• Identify and blacklist problem IPs (external)

IH:
• Remediate vulnerabilities and threats
Scenario Wrap Up – Review Stage 3

CDAP:
- Identify problem areas that allowed for SQL Injection
- No data validation on web page
- Vulnerable SQL server

CND:
- Identify user machine and external IP talking via IRC
- Find SNORT alerts relating to IRC and SQL Inject

IH:
- Remediate vulnerabilities and threats
Scenario Wrap Up – Review Stage 4

CDAP:
- Stop exfiltration attacks from occurring
- Determine where malware originated (internal IP address)

CND:
- Detect 3 exfiltration attempts: easy/med/hard
- What type? Any payload/file?
- Internal/External IPs
- Identify a DoS occurring from inside the network
- Source and destination IPs (ipv6?)
- Identify malware on the network

IH:
- Remediate vulnerabilities and threats
- Identify malware (malicious PDF)
Conclusion

On behalf of Carnegie Mellon University, the Software Engineering Institute, and the CERT Enterprise and Workforce Management Directorate, thank you for your time today.

Brian D. Wisniewski
Lead Cyber Security Developer & Trainer

bdwisniewski@cert.org
Notices

© 2012 Carnegie Mellon University
This material is based upon work supported by the U.S. Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® is a registered mark owned by Carnegie Mellon University.