TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Maintaining a 24/7 Army Information Assurance Workforce: Lessons Learned from a Researcher's Perspective

Mr. Curtis Arnold

24 March 2010

Read-Ahead

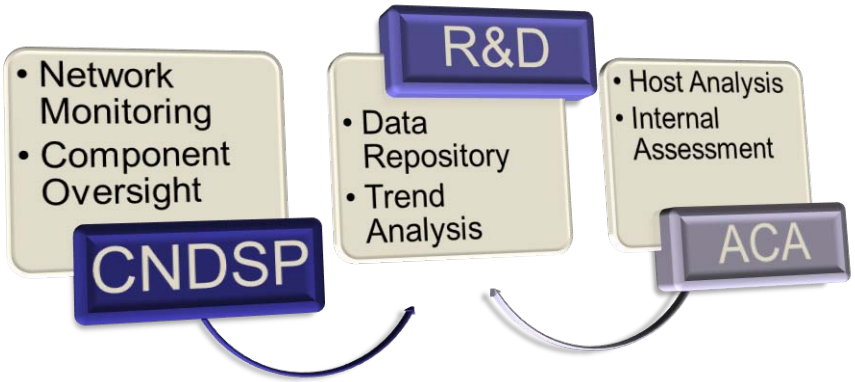
- Objectives
- Organizational Background
- Foundation Training
- Skills Analysis
- Skills Matrix
- Example Skill Training Plan
- Lessons Learned

Objectives

- Discuss skills required in a large Information Assurance (IA) organization
- Identify cross-training for multiple skills
- Show example of multiple training methods for one skill

Organizational Background

Sustaining Base Network Assurance Branch (SBNAB)



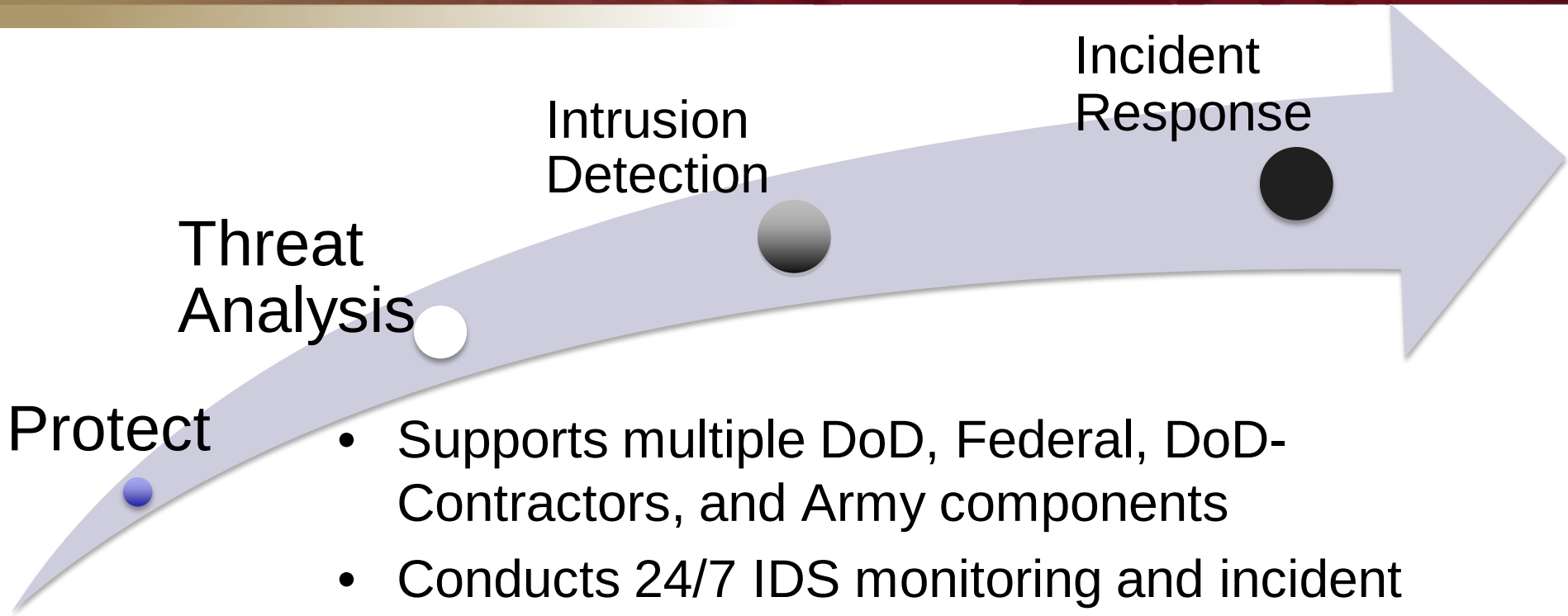
Gather and make available multiple types of data for the R&D community

The R&D team is responsible for not only maintaining the data, but also performing internal research in support of Cyber Initiatives

There are two operational components to support the collection of data

- **Computer Network Defense Service Provider (CNDSP)** – Primarily responsible for collecting network or external datasets
- **Agent of the Certification Authority (ACA)** – Responsible for collecting internal datasets, such as scan results, host configurations, and Access Control Lists (ACLs)

Computer Network Defense Service Provider (CNDSP)



- Supports multiple DoD, Federal, DoD-Contractors, and Army components
- Conducts 24/7 IDS monitoring and incident reporting
- Protect services include compliance monitoring and oversight
- Supports R&D mission by collecting network data

Agent of the Certification Authority (ACA)

- Core Government agencies that provide independent Certification & Authentication (C&A) validations
- Average over 80 assets per year
- Supports the R&D mission by collecting internal data to include:
  - Access Control Lists (ACLs)
  - Vulnerability scans
  - Training status
  - Host configurations

Training

Research & Development

Network Monitoring & Response

Certification & Accreditation (C&A) Validations

Foundation Training

DoD 8570.01 – Information Assurance Workforce Improvement Program provides a good foundation

Due to our diverse set of responsibilities and cross-training additional skills are needed

Setting the Stage

In order to maximize our training we had to implement a few rules such as:

- Government and Contractor staff had to meet the same standard except for some Federal courses that are Government only
- Training had to be from a reputable source
- Training had to be cost effective and include a mixture of:
  - On-The-Job (OTJ) training
  - College Courses
  - Federal programs (OPM Leadership)
  - Vendor training

Skills Analysis

Business

- Leadership Skills
- Cost Formulation
- Business Writing
- ROI Analysis

Technical

- DoD Specific Tool Sets
- Security Engineering
- Secure Coding
- Vulnerability Scanning
- Packet Analysis

Policy

- Policy and Procedure Development
- Risk Analysis
- Conduct IA training
- Compliance Reporting

Skills Matrix

	Leadership	Cost Formulation	Secure Coding	Policies and Procedures	Risk Analysis	Vulnerability Scanning	Conduct IA Training
CND Manager	D	D	K	D	D	M	K
CND Senior Analyst	D	D	K	M	D	M	M
CND Junior Analyst	K	K	M	D	D	M	K
ACA Manager	D	D	K	D	D	M	M
ACA Assessor	M	K	M	D	D	D	M
Senior Software Developer	D	M	D	M	M	M	M
Senior System Admin	D	M	M	M	M	D	M

Legend:
D = Can perform this skill on a daily basis
M = Can perform this skill on a monthly basis
K = Must have knowledge of this skill for day-to-day operations

Example Training

Example Skill: Packet Analysis

Target Audience: CND Junior Analyst

Beginning skill level: Some knowledge of packets, OSI Model, etc…

Training Plan:

1. Read two standard books on the subject
2. Receive training from Senior Analyst
3. Practice analysis on test data
4. Six month window with all analysis reviewed by Senior Analyst
5. Complete advanced college course that addresses this subject

Lessons Learned

- ***Technical*** training has to be directed at specific skills, while ***Policy*** training needs to be more diverse
- ***Multiple*** training mediums must be used to meet long and near term needs
- Type and amount of training is ***closely monitored*** by all employees, which means it must be applied equally
- Employees must be ***held responsible*** for staying current in their professional area

QUESTIONS???

CONTACT INFORMATION:

CURTIS ARNOLD
U.S. ARMY RESEARCH LABORATORY (ARL)
CURTIS.B.ARNOLD@US.ARMY.MIL
301-394-0263