Job Performance Model for Advanced Threat Responders

ROBERT HUBER

CRITICAL INTELLIGENCE

MICHAEL ASSANTE

NBISE

Session ID: DAS-304

Session Classification: General Interest

RSACONFERENCE2012

What is a Cyber Defender?

- Do you know what skills are required to be an effective Cyber Defender?
- Do you know how to defend against Advanced Persistent Threats?
- What do you look for in a prospective new hire?

Objectives

- Best practices for the development of monitoring, detection, prevention, response and policy approaches to address advanced threats
- Identify key goals associated with functional cyber security roles instrumental in responding to advanced threats
- Understand technical task overlaps between functional roles
- Analyze technical skills by their impact to mission accomplishment and as differentiators of skilled performance from novice through master

How Do We Do That?

- Mike –insert the entire workflow/process here; however many slides that takes

Future of Utilizing the Competency Models

- Modular assessment or test design
  - Adaptive, goal-driven test sequences assess aptitude, knowledge, skill, and ability to perform a specific task
  - Validated pools of test scenarios/questions for constructing randomized, equivalent test forms
- Modular simulation exercises
  - Validated, simulation routines for modeling, practicing, and assessing specific skilled behavior
- Modular curriculum design
  - Validated content packages for accomplishing specific learning objectives

How is the NBISE Approaching Competency Differently?

- Context elicitation through vignettes and responsibilities
- Competencies defined at novice, apprentice, journeyman, and expert levels for multiple roles (organizational language)
- Creating profiles for technical and operational skills
- By defining assessments at the task level we create reusable libraries to assess multiple roles
- ADAPTS validation and extension of job performance model
- Standards based on validated curricula, assessment, and simulation libraries

Job Task Competency Analysis (JTCA)

- Funded by DOE Grant for Workforce Development, performed by NBISE
- 10 Panel Members, over 75 years of security experience
- Intended to identify the knowledge, skills and abilities (KSAs) necessary to detect and respond to targeting and exploitation by sophisticated threat actors
- Analyze technical skills by their impact to mission accomplishment and as differentiators of skilled performance from novice through master

JTCA

- Vignettes
  - Incident Description
  - Primary Problem
  - Entities involved
  - Systems involved/affected
  - Roles/Titles involved/affected

JTCA - Vignette

- Incident Description: Internal workstation attempting highly abnormal, direct-to-Internet connection bypassing the organization's outbound proxy infrastructure. Communication noticed via core traffic analysis within SIEM Flow traffic.

  Primary Problem: Traffic typically indicative of infected internal system (malware) and Security Analyst escalates the activity as such after performing some rudimentary analysis. the unknown workstation's traffic not being seen in proxy infrastructure. Remote AV scan of internal system shows no infection. After further analysis of the Flows, destination IP, etc. by Engineering, the system is determined to be a visiting vendor's own laptop attempting to automatically update an application installed on that system. The vendor uses no proxy at home nor in the office, and therefore wasn't configured to destin through any proxy. The traffic was being dropped before it hits the proxy infrastructure and, therefore, not seen on border packet and capture technology.

  ==
  Entities involved/affected:
  Security Operations
  Security Engineering

  Systems involved/affected:
  Web proxies
  Packet and capture technology
  Workstation AV
  Internal SIEM

  Roles/Titles involved/affected:
  Security Analyst
  Security Engineer

JTCA – Role Definition

IT Security

- 15. IDS Administrator
- 28. Security Architect
- 27. Information Systems Security Engineer
- 24. IS Analyst
- 21. IT Security Firewall Admin
- 29. Incident response
- 32. vulnerability managers
- 48. Security SOC
- 44. Firewall engineers
- 42. Intrusion Response Analysts
- 38. Security incident response
- 40. Security engineering

JTCA – Roles To Responsibilities

IT Security

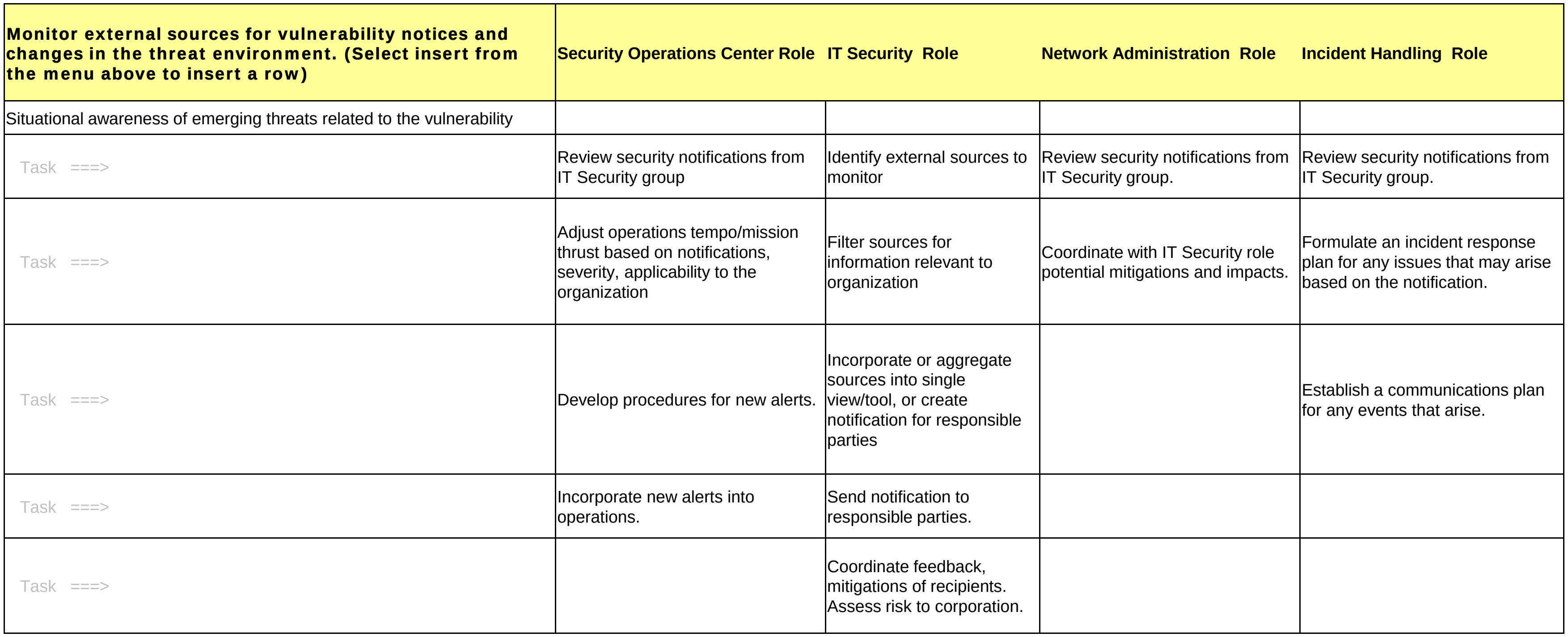
- Need to get this data

JTCA – Map Roles To Outcomes

Vignettes	Security Operations Center Role	IT Security Role	Network Administration Role	Incident Handling Role
Vignette: SQL injections observed via normal monitoring	Detected SOC has procedures to deal with these events, and/or reviews their current proedures	Blocked Provide 2nd level analysis of event from SOC	Blocked Provide router logs and netflow data to IR team	1. Detected, mitigated, and investigated 2. System returned to operation 3. Lessons learned applied
Vignette: Compromise of data through poor security practices.	Detected SOC has procedures to deal with these events, and/or reviews their current proedures SOC engages IR for response	New signatures Provide 2nd level analysis of event from SOC	Blocked at gateways Provide router logs and netflow data to IR team	1. New incidents detected 2. Analysis, forensics, mitigations coordinated 3. System returned to operation 4. Lessons learned applied
Vignette: A large company's network was compromised and intellectual property was stolen.	Detected Procedures for these events are validated, or updated IR is engaged	Blocked at gateways Provide 2nd level analysis of event from SOC	Blocked Provide router logs and netflow data to IR team	1. Detected, response, investigated 2. Analysis, forensics, mitigations coordinated 3. System returned to operation 4. Lessons learned applied

JTCA – Mission Definition or Goals to Resp.

- Need to get this

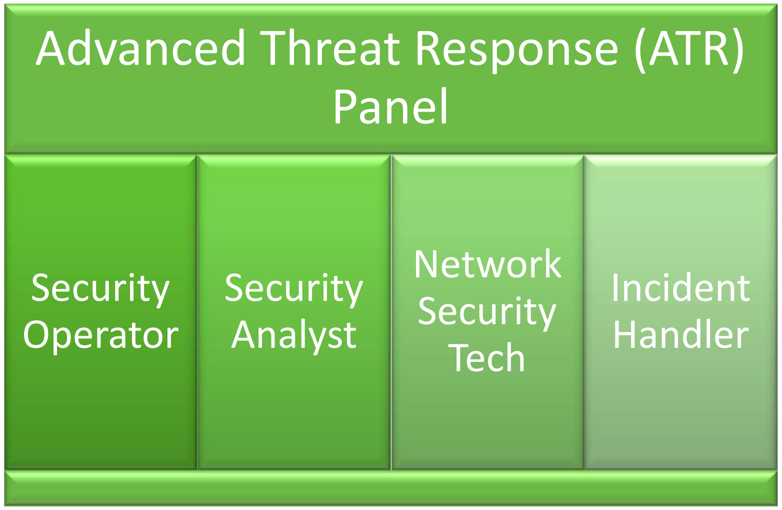


Monitor external sources for vulnerability notices and changes in the threat environment. (Select insert from the menu above to insert a row)	Security Operations Center Role	IT Security Role	Network Administration Role	Incident Handling Role
Situational awareness of emerging threats related to the vulnerability				
Task ===>	Review security notifications from IT Security group	Identify external sources to monitor	Review security notifications from IT Security group.	Review security notifications from IT Security group.
Task ===>	Adjust operations tempo/mission thrust based on notifications, severity, applicability to the organization	Filter sources for information relevant to organization	Coordinate with IT Security role potential mitigations and impacts.	Formulate an incident response plan for any issues that may arise based on the notification.
Task ===>	Develop procedures for new alerts.	Incorporate or aggregate sources into single view/tool, or create notification for responsible parties		Establish a communications plan for any events that arise.
Task ===>	Incorporate new alerts into operations.	Send notification to responsible parties.		
Task ===>		Coordinate feedback, mitigations of recipients. Assess risk to corporation.		

JTCA –

Goal	Priority	Objective measure	Premier	Robust	Improved	Satisfactory	Moot
Update overarching policies and procedures	Primary	The time frame policies and procedures are updated to reflect the changing threat landscape	Policies and procedures are updated in real time as incidents are worked and new threats are discovered	Policies and procedures are updated weekly to reflect incidents worked that week and new threats discovered that week	Policies and procedures are updated monthly to reflect incidents worked that month and new threats discovered that month	Policies and procedures are updated every 6 months to reflect incidents worked during the previous 6 month period and new threats discovered during that same 6 month period	Policies and procedures are updated annually to reflect incidents worked during the year and new threats discovered during the year
Perform gap analysis of ability to detect or identify vulnerable systems	Primary	Time frame required to determine gaps	Gap analysis performed within 1 hour of vulnerability notification	Gap analysis performed within 2 hours of vulnerability notification	Gap analysis performed within 4 hours of vulnerability notification	Gap analysis performed within same working day of vulnerability notification	Gap analysis performed after 24 hours
Monitoring sources for vulnerability notices and changes in the threat environment	Primary	Person/Resource assigned task to monitor sources	Dedicated threat intelligence team Automated solution to monitor and provide information automatically to team based on asset profiles, or risk profiles of members	Dedicated threat intelligence resource Automated solution to monitor and provide information automatically to team	Resource assigned additional threat intelligence responsibility Automated solution to monitor and provide information for manual review	Automated solution to monitor and provide information for review	No resources to monitor
Respond to intrusion events	Primary	Monitor security events real time	24x7 security staff monitor security events real time	8x5 security operations staff monitor events near real time	Security events are sent to personnel automatically near real time	Security events are reviewed manually as time permits	No capability to monitor security events

Advanced Threat Response (ATR)



Advanced Threat Response (ATR) Panel

Security Operator

Security Analyst

Network Security Tech

Incident Handler

ATR Panel is focused on advanced cyber security threats such as advanced persistent threats and other highly-sophisticated threat vectors.

- Completed work for 4 job roles
- Identified 706 technical tasks

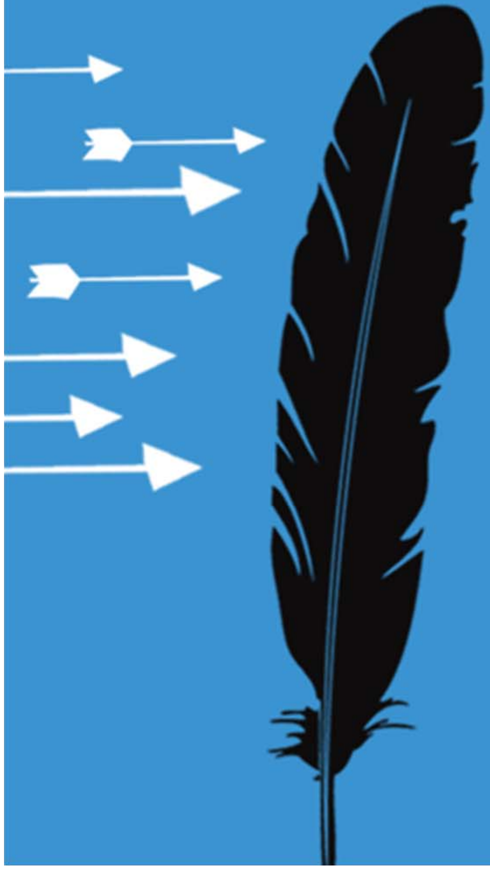
ATR Draft Competency Model –INSERT INTEL TASKS HERE

Goals and Example Responsibilities (631 unique tasks)

Constructs	Constructs
Monitor security events internally (92) •Monitor for such policy violations and report up as necessary •Detection of malicious traffic •Monitor for compromises	**Perform gap analysis of ability to detect and respond to vulnerabilities (32)** •Assist in determining patch release timelines based on associated risk. •Coordinate mitigation and detection techniques among all groups •Develop a notification / alert to be disseminated to all relevant parties.
Monitor external sources for vulnerability notices and changes (12) •Filter sources for information relevant to organization •Coordinate with IT Security role potential mitigations and impacts. •Formulate an incident response plan for any issues that may arise based on the notification.	**Respond to intrusion events (255)** •Determine scope of incident •Interface with law enforcement •Determine root cause
Create and implement safeguards and countermeasures (163) •Update relevant detection mechanisms •Write/test/deploy/tune signature •Update antivirus and IDS signatures	**Update overarching policies and procedures (77)** •Ensure operational procedures updated to respond to new alerts •Review effectiveness of procedures/policies for system implementation •Determine if there is a valid and required need for the access

What can you do today? How can you benefit or contribute?

- Become a panel member
- Participate in the JAQ
  - Contact me or NBISE and specify the ATR Panel
- Utilize the assessment tools developed by NBISE
- Participate in other NBISE Panels (SmartGrid, OST)



Divider Slide Type Section Title Here

RSACONFERENCE2012

Apply Slide

- Bullet point here (see slides 4 and 5 for instructions)
- Bullet point here
- Bullet point here