Positioning the National Guard and Civilian Organizations to Augment the Cybersecurity Workforce

June 21, 2017
National Guard Cyber

LTC Brad Rhodes
21 June 2017
Outline

• National Guard Bureau
• Colorado Army National Guard Cyber Teams
• CPT and DCO Comparison
• Exercises & Kinetic Cyber Demo
• Training & Certifications
National Guard Bureau

The Joint Staff

Public Private Partnerships
Coordinate, Train, Advise & Assist
Relationship Building BEFORE an Incident
Colorado Army National Guard Cyber Teams

Cyber Protection Team (CPT) 174

Defensive Cyber Operations-Element (DCO-E)
CPT and DCO-E Comparison

DCO-E
- Defends the Guard Enterprise
- Systems Focused
- High ROI Enterprise Security
- Vulnerability Centric
- Trained for General Defense and Response
- Guided by CIO
- Cyber Train/Advise/Assist
- Fixed Position
- Support to NIPR/SIPR
- Foundation – Title 40 U.S.C
- T32 / SAD Only

Joint Core
- Vulnerability Scanning
- IAVA Validation
- Compliance Assessment
- Metrics Reporting
- Intelligence Review
- Tactical SME Support

CPT
- Defends a Mission
- Key Terrain Focused
- High ROI Mission Security
- Threat Centric
- Trained Specific Threats
- Trained for Specific Terrain
- Executes CCDR/Svc Mission
- OPLAN/CONPLAN Assignable
- Support beyond NIPR/SIPR
- Deployable
- Foundation – Title 10 U.S.C.
- T32 / T10 / SAD (possible)

118 CN DSP Tasks Validated
DODI 8530.01aa and ESM v8

Protect • Monitor, Analyze & Detect • Respond • CND Sustainment

*Computer Network Defense Service Provider
Exercise & Kinetic Cyber Demo

- Dam Simulator Vulnerabilities
- Rogue Access Point
- WAP with a Critical Vulnerability
- Attack Vectors
- Live Exploits
- Aftermath...

Engagement with Mission Partners including: State, County, Local Governments; Academia; Critical Infrastructure Owners; Industry
Certifications & Training

DoD 8570-M (soon to be replace by DoD 8140-M)

<table>
<thead>
<tr>
<th>IAT Level I</th>
<th>IAT Level II</th>
<th>IAT Level III</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSCP</strong></td>
<td><strong>SSCP</strong></td>
<td><strong>CISSP (or Associate)</strong></td>
</tr>
<tr>
<td>A+ CE</td>
<td>CCNA-Security</td>
<td>CASP</td>
</tr>
<tr>
<td>CCNA-Security</td>
<td>GSEC</td>
<td>CISA</td>
</tr>
<tr>
<td>Security+ CE</td>
<td>Security+ CE</td>
<td>GCED</td>
</tr>
<tr>
<td><strong>IAM Level I</strong></td>
<td><strong>IAM Level II</strong></td>
<td><strong>IAM Level III</strong></td>
</tr>
<tr>
<td><strong>CAP</strong></td>
<td><strong>CAP</strong></td>
<td><strong>CISSP (or Associate)</strong></td>
</tr>
<tr>
<td>GSLC</td>
<td>CCNA-Security</td>
<td>CASP</td>
</tr>
<tr>
<td>Security+ CE</td>
<td>GSEC</td>
<td>CISA</td>
</tr>
<tr>
<td><strong>IASAE I</strong></td>
<td><strong>IASAE II</strong></td>
<td><strong>IASAE III</strong></td>
</tr>
<tr>
<td><strong>CISSP (or Associate)</strong></td>
<td><strong>CISSP (or Associate)</strong></td>
<td><strong>CISSP-ISSAP</strong></td>
</tr>
<tr>
<td>CSSLP</td>
<td>CSSLP</td>
<td>CISSP-ISSAP</td>
</tr>
<tr>
<td>CASP</td>
<td>CASP</td>
<td>CISP</td>
</tr>
<tr>
<td><strong>CND Analyst</strong></td>
<td><strong>CND Infrastructure Support</strong></td>
<td><strong>CND Incident Responder</strong></td>
</tr>
<tr>
<td>CEH</td>
<td>CCNA</td>
<td>CEH</td>
</tr>
<tr>
<td>GCIA</td>
<td>GFI</td>
<td>CISA</td>
</tr>
<tr>
<td>GCIH</td>
<td>GFA</td>
<td>GCED</td>
</tr>
<tr>
<td><strong>CND Auditor</strong></td>
<td><strong>CND-SP Manager</strong></td>
<td></td>
</tr>
<tr>
<td>CEH</td>
<td>CISSP-ISSMP</td>
<td>CISM</td>
</tr>
<tr>
<td>GCIA</td>
<td>CISM</td>
<td>CISP</td>
</tr>
<tr>
<td>GCIH</td>
<td>GCED</td>
<td>GCIA</td>
</tr>
</tbody>
</table>

Training Sources:
- Cyber Center of Excellence (Fort Gordon, GA)
- National Guard Professional Education Center
- Cyber Center of Excellence Mobile Training Teams
- Academia
- Contracted (e.g. SANS Institute)

Cyber Exercises:
- Cyber Shield (National)
- Cyber Guard (National)
- Cyber Yankee (Regional)
- Local/State (e.g. Vital Connection in Colorado)

Many Soldiers from industry with skills such as: Penetration Testing, Coding, Auditing, Systems Administration, Systems Engineering, Network Security, Routing and Switching, Application Development, etc…
Contact

LTC Brad Rhodes

• Email: brad.e.rhodes.mil@mail.mil
Q & A
Michigan Army National Guard Cyber Operations
Training Approach

- Army and Air Guard train in similar fashion
- Often we attend exercises with a joint team (Cyber Shield 2018 we expect to take a multi agency team)
- Both teams are stretched thin and recruiting and training as fast as we can
- Army is currently working toward recruiting 150% - 200% strength
Michigan Army National Guard
Task Organization

**Defensive Cyber Operations Element**
- Team Chief: LTC 25G
- Team Chief: MAJ 25G
- Asst Team Chief: CPT 01A
- Asst Team Chief: CPT 01A
- Info Service Tech: W2 255A
- Info Protection Tech: W3 255S
- Network Mgmt Tech: W2 255N
- Incident Responder: MSG 25D
- Incident Responder: SFC 25D
- Info Tech Specialist: SSG 25B
- All Source Intel Analyst: SSG 35F

**Cyber Support Squad**
- CND Manager: CPT 17A
- Systems Architect: W2 255A
- Systems Architect: W2 255A
- Network Infrastructure Service Specialist: W3 255N
- Cyber Security Analyst: SFC 25D
- Close Access Network Operator: SSG 25D
- All Source Intelligence Analyst: SGT 35F

**Mission Protection Squad**
- CND Manager: CPT 17A
- Cyber Ops Officer: W2 170A
- Systems Architect: W2 255A
- Network Infrastructure Service Specialist: W2 255N
- Cyber Security Analyst: SFC 25D
- Close Access Network Operator: SSG 25D
- All Source Intelligence Analyst: SSG 35F
Training Approach

Though we have distinct Task Organization, the we (Army) view our 3 sections as one team and train everyone to function on all teams.

Advantages:
• Can leverage expertise across the teams for internal training
• Allows Leadership to spread the wealth when ad-hoc missions come down
• Team is exposed to wide range of training

Disadvantages:
• Training may not be as in depth as it may otherwise be
• Team is expected to maintain a broader range of knowledge
Support in Michigan

Defend the Guard Military Network in Michigan
- We can be activated to supplement the full time organization if the need arises
- By doctrine, this is the mission of the DCO-E. However, we reach across all teams
- We were recently activated to respond to an incident

Support Local Industry
- State Police are the lead agency
- Guard can be activated by the Governor using State Active Duty funding
- Guardsmen can only Coordinate, Train, Assist, and Advise
- We have been activated one time to assist a hospital during the Flint Water Crisis
External Support

Federal Government
• Members of the National Guard can be activated under Title 10
• By doctrine, this is the mission of the CPT
• Currently have 9 pax on Title 10
• Will not necessarily mobilize a total unit, may ask for eaches
• Annual rotations for the foreseeable future

Challenges
• Security Clearances – Top Secret takes a year or more to get approved
• Amount and length of training
  ➢ Takes roughly 2 years to train a Warrant Officer
  ➢ Takes roughly 15 months +/- to train a Cyber Operations Officer
• Retention – private sector wants our people as they are highly skilled
Contact Data

Major Robert A. Maciolek, Team Chief, Defensive Cyber Operations, Michigan Army National Guard

Army: robert.a.maciolek2.mil@mail.mil

Civilian: mac@staticlinesoftware.com
Q & A
Michigan Cyber Civilian Corps

21 June 2017

Ray Davidson PhD, CISSP, GIAC 0x0B
MiC3: Overview

Information security professionals who volunteer to provide expert assistance to enhance the State’s ability to rapidly resolve cyber incidents when Activated under a Governor declared State of Emergency

• Operate under state Cyber Disruption Response plan
• Legislation in process
  • Provides tort immunity; indemnity
  • Lower threshold to Activate
  • Provide for Advisory Board
• Community Service
MiC3: Overview

Unique:
- Only state sponsored all-volunteer force of cyber defenders (to date) (that we know of!)
- 56 Members (as of today; 200 by YE 2018)
- Half of members meet DoD Directive 8570 for skills Certifications (GCIH and others)
MiC3: Requirements to Apply

• Members must have:
  - At least two years of information security, incident response, and/or digital or network forensics
  - One foundational Security certification
    - (Security+, C|EH, CISSP, or GIAC, etc.)
  - 10 days of support from employer (a signed letter of agreement is required)
  - 5-6 days for training, 1-2 exercises, community volunteering, etc. (weekends possible in the count)
MiC3: Membership Requirements (1)

Pass a series of Security Competency Assessments

• Series of tests to demonstrate basic and advanced knowledge of networking and security concepts, as well as basic IR (Incident Response) and Forensics skills
Background Check

“Ten-Print” (FBI National) background check

Confidential Disclosure Agreement

To address potential conflicts of interest
MiC3: Membership Benefits

Training

- Significant Training Opportunities
  - 2016: SANS SEC504, 2017: SANS SEC511
  - Collaboration with National Guard & State Police

Prof Dev

- Networking throughout Michigan
- Collaboration with IT security professionals across multiple economic verticals, industries, the academy, public sector, local government, and private sector

Civic Duty

- Providing members a platform to aid the state in crisis (or preventing it!) while doing what they love
Governor Rick Snyder’s idea: MiC3, announcement at 2013 North American International Cyber Summit.

Partnership between the State of Michigan, the Merit Network Inc., and Mich Health and Humans Services.

Decision was made to consolidate the program management with the State of Michigan, with Merit as a partner.

MiC3: Calendar

Quarterly

Face-to-Face Meeting

Monthly

MiC3 Conference Call: All Members, Executive Sponsor, Staff

Planned 2017 Events

April 12

Ferris State University Day-Long and Exercise

July 24-29

SANS Training SEC511

October 30

North American International Cyber Summit
• **Contacts**
  - Ray Davidson, Ph.D., CISSP, ETC (Program Manager)  
    DavidsonR5@michigan.gov, ray@kzodavidsons.org Twitter: @raydavidson  
  - Patrick Chandler (Project Coordinator) - ChandlerP@michigan.gov  
  - Paul Groll, MS, CISSO, CISSP, CCSE (Executive Sponsor) - GrollP@michigan.gov

• **Links**
  - [MiC3 Website](https://www.micybercorps.org)
Q & A