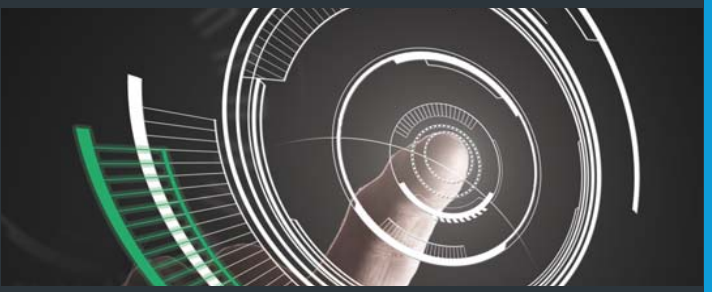
Current Use Cases

- CCRI
  - Network Traffic Analysis
  - Legacy OS Detection
  - Banned Port and Protocol Usage
  - Misconfigured Perimeter Devices
  - Misconfigured CDS
- CCORI
  - Network Traffic Analysis
  - Legacy OS Detection
  - Port and Protocol Usage
  - Misconfigured Perimeter Devices
  - Misconfigured CDS
  - Proper IP Reporting
- Insider Threat
  - Big Data Exfiltration
  - Destination of Traffic IP
  - Single IP Traffic Analysis
- ADHOC Analysis
  - IP Utilization
  - Proper IP Reporting
  - Ports and Protocol Verification

Potential Use Cases

- CMRS validation
  - Big Data exploitations and analysis
  - OS & application identification
  - Protocol Verification (non-web traffic using port 80)
  - Protocol Negotiation (SSHv1 vs SSHv2, RC4 vs AES-256)
- Enclaves with open servers
  - Open mail relays
  - Open web proxies
- Peer to Peer activity between user enclaves
- RFC 1918 compliance/backside connections



Possible Future Capabilities

- Penetration testing (Limited)
- Threat hunting (Limited)
- Targeted compliance hunting

Compliance Monitoring Team:

Phone (Commercial): (301) 225-2902
Phone (DSN): (312) 225-2902
Email (NIPR): disa.meade.re.mbx.caoscans@mail.mil
Email (SIPR): disa.meade.ns.mbx.caoscans@mail.smil.mil

Hours Of Operation: 0700-1700 EST

CHA provides Compliance Overview of the following:

DoDI 8551 Ports, Protocols, and Services Management (PPSM)
http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf

DISN Connection Process Guide (CPG)
http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide

CJCSI 6211.01D Defense Information System Network Responsibilities
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02a.pdf

DoDI 8510 Risk Management Framework (RMF) for DoD Information Technology (IT)
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

For more information:

DISA Risk Adjudication and Connection Division Web
http://www.disa.mil/network-services/enterprise-connections

Acropolis Suite:
http://www.disa.mil/Cybersecurity/Analytics/Acropolis

CHA Mission Partner Information Paper:
https://disa.deps.mil/org/RE4/RE41/NSC1External%20Documents/Forms/AllItems.aspx

DISA

Connection Approval Branch
Compliance Monitoring Team (CMT)

Connection Approval Branch
Compliance Monitoring Team

Mission

The Risk Adjudication Division's Connection Approval Office/Branch (RE41) conducts Cyber Hygiene Analysis (CHA) to analyze the enclave's cybersecurity health. Combined data from active and passive tools give a "snapshot" of an enclave's security posture in accordance with DOD compliance requirements.

Functions

The Compliance Monitoring Team (CMT) conducts a CHA with the intent of examining vulnerabilities and compliance in accordance with Security Technical Implementation Guides (STIGs), Information Assurance Vulnerability Management (IAVM), and policies.

- Analyze captured passive Acropolis data for:
  - Banned data services
  - Legacy operating systems
  - IP optimization/utilization
  - Persistent characteristic analysis
- Utilize ACAS/NESSUS scan data for
  - Perimeter Defense Testing
  - Vulnerability Assessment
- Cross Domain Solution (CDS) advertising verification
- System of Record verification, SGS/GIAP & SNAP registration verification

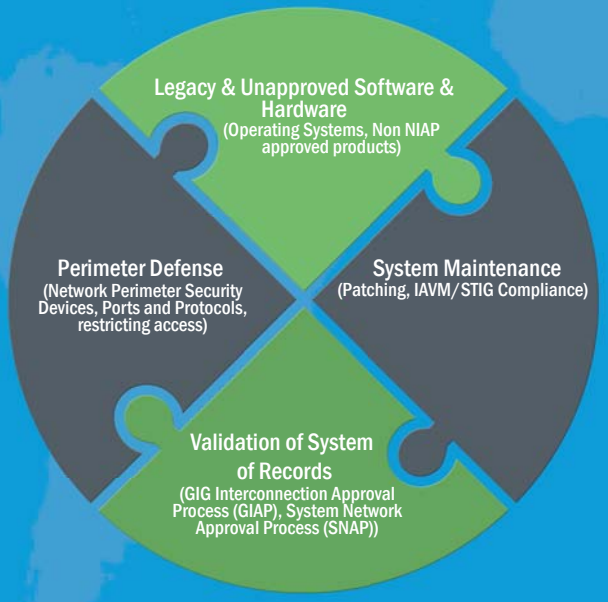
Who Could Benefit from a CHA?

- Authorizing Official (AO)
- Information System Security Manager (ISSM)
- Chief Information Security Officer (CISO)
- Enclave Owner (EO)
- Compliance Auditor/Inspection Lead

What Does a CHA Offer?

- Offers enclave owners an opportunity to improve their enclave's cyber security posture
- Proactively discovering and resolving security violations affecting Confidentiality, Integrity, and Availability
- Provides an enhanced holistic view of enclave's hygiene

Hygiene



Benefits of a CHA?

- Provide enclave health assessment prior to CCRI inspections
- Provide service/product to inspection teams to benefit inspection processes
- Offer enclave owners opportunity to improve their enclaves' cybersecurity posture
- Constructive resolution to help customers pass CCRI

Current Toolset

Acropolis – Passive Tool

Currently collects, stores, and analyzes both enclave and backbone network traffic on the Non-secure Interpret Protocol Router Network (NIPRNet) at the Aggregated Routers (AR) and the Internet Access Point (IAP) on the Secret Internet Protocol Router Network (SIPRNet) at the Perimeter Edge Routers (S-PE).

- **SiLK (Netflow)**
  - Queries large historical data sets for trend analysis
  - Identifies potential PPSM violations for a specific time period
- **Trickler (OS Fingerprinting)**
  - Identifies hosts within an enclave for situational awareness and to tailor other scan activities
- **Noesis (Packet Capture)**
  - Provides detailed analysis of specific data session
  - Can provide login credentials passed in clear text (e.g., Telnet, FTP)

ACAS (Assured Compliance Assessment Solution) NESSUS – Active Tool

- Enterprise DoD Tool
- Active Nessus and Passive Vulnerability Scanner (PVS)
- Identifies Information Assurance Vulnerability Management (IAVM) and Security Technical Implementation Guide (STIG) compliance for some host-based vulnerabilities