CERIAS

The Center for Education and Research in Information Assurance and Security

Centralized Hierarchical Cybersecurity Monitoring Towards Securing the Defense Industrial Base Supply Chain

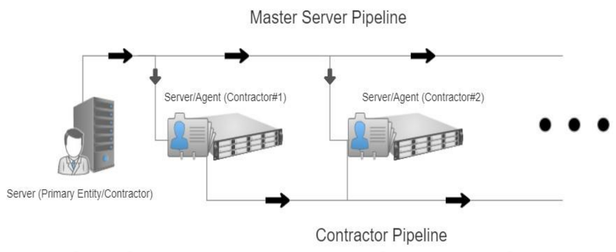
Vijay Sundararajan, Dr. J. E. Dietz

Contact: sundar17@purdue.edu, +1-765-428-0879

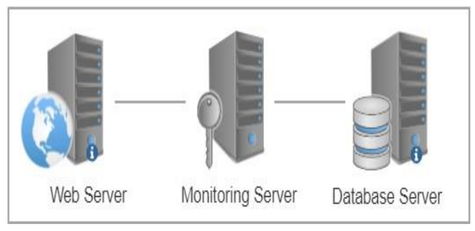
Motivation

The implementation of the Centralized Hierarchical Cybersecurity Monitoring (CHCM) model was motivated by the critical need to meet stringent cybersecurity compliance regulations within the Defense Industrial Base (DIB) supply chain. CHCM aimed to provide a comprehensive, **centralized, near real-time solution** to ensure end-to-end protection of Controlled Unclassified Information (CUI) and mitigate cybersecurity risks effectively. Safeguarding CUI and confidential communications **throughout the supply chain**, from the DoD to its contractors/sub-contractors, is imperative to mitigate cyber threats. The model is applicable to any type of supply chain relying on information systems to transfer important information and data.

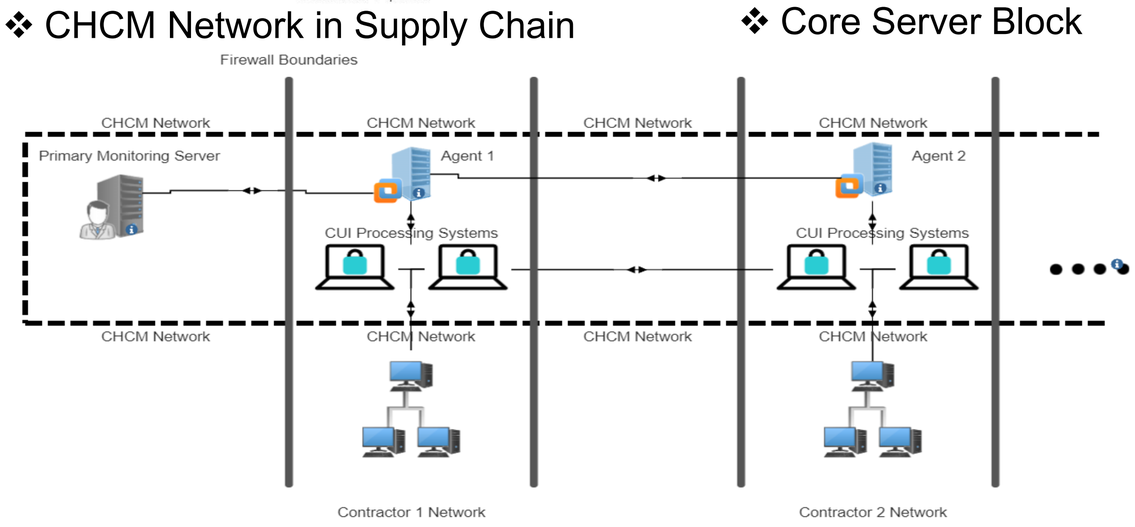
CHCM Framework



❖ CHCM Network in Supply Chain



❖ Core Server Block

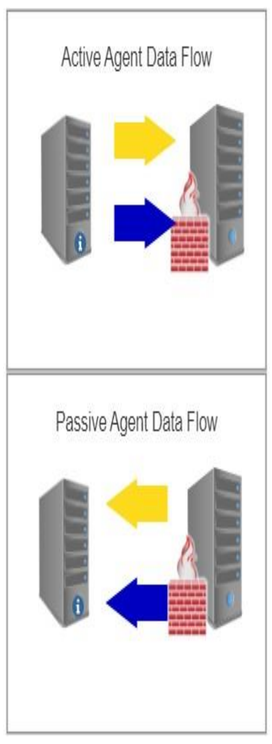


❖ CHCM Network imposed on an organizational network infrastructure

Working and Operation

- The CHCM network operated on a server-agent or master-slave hierarchical model, with master servers overseeing supply chain compliance and contractor servers monitoring and maintaining sub-agents' compliance.
- Endpoint telemetry was communicated to the CHCM server for analysis and decision-making, facilitating real-time feedback and automation through active and passive proxies.
- VPN access, Multi-Factor Authentication (MFA), and zero-knowledge end-to-end encryption ensured secure communication within the CHCM network, while firewalls and Access Control Lists (ACLs) were used to enforce security rules.
- Internal network testing, external penetration testing, log monitoring, and social engineering tools were employed to monitor, detect, and address vulnerabilities, with an emphasis on automation for prompt remediation.

❖ Agent –Server Data Flow



❖ Automation algorithm for external vulnerabilities

Algorithm 1 Automated Vulnerability Discovery

Input: *subnet* ▷ Target subnet or IP range
Input: *intensity* ▷ Scan intensity level
Input: *outputDir* ▷ Directory for results
procedure VULNERABILITYDISCOVERY
  nmap ← Initialize with *subnet* and *intensity*
  activeHosts ← Discover hosts with *nmap* -sn
  for all *host* in *activeHosts* **do**
    ports ← Scan ports of *host* with *nmap* -sV
    vulnData ← Execute Vulners script on *ports*
  end for
  Save *vulnData* to *outputDir* in XML or HTML
  POSTPROCESS(*vulnData*)
  ALERTIFNEEDED(*vulnData*)
end procedure
procedure POSTPROCESS(*data*)
  Parse and summarize *data* for report
end procedure
procedure ALERTIFNEEDED(*data*)
  Check *data* for critical vulnerabilities
  Trigger alerts for any findings
end procedure

Results From 9 DoD Contractors

❖ Results taken in the fiscal year 2020 with regular periodic monitoring

TABLE I: Cybersecurity Monitoring Metrics for the Year 2020 - Periodic

OrgNo	Internal	External	Log Alerts	SE	Compliance %
Org 1	6	4	16	3	65
Org 2	5	4	12	1	70
Org 3	8	3	23	3	60
Org 4	10	5	19	2	75
Org 5	6	3	8	0	72
Org 6	7	1	27	1	58
Org 7	8	2	34	2	68
Org 8	4	3	10	0	80
Org 9	7	2	7	1	85

❖ Results taken in the fiscal year 2021 with CHCM framework

TABLE II: Cybersecurity Monitoring Metrics for the Year 2021 - CHCM

OrgNo	Internal	External	Log Alerts	SE	Compliance %
Org 1	4	3	1	1	85
Org 2	3	1	3	2	88
Org 3	5	0	2	1	83
Org 4	2	1	0	0	92
Org 5	4	2	4	1	90
Org 6	5	3	0	2	82
Org 7	4	1	3	0	87
Org 8	1	1	0	1	94
Org 9	2	0	1	0	97

PURDUE UNIVERSITY

CERIAS