



# Distributed Security Operations Use Case

Roman Danyliw <[rdd@cert.org](mailto:rdd@cert.org)>

MAMI Management and Measurement Summit (M3S)

March 16, 2018

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-0355

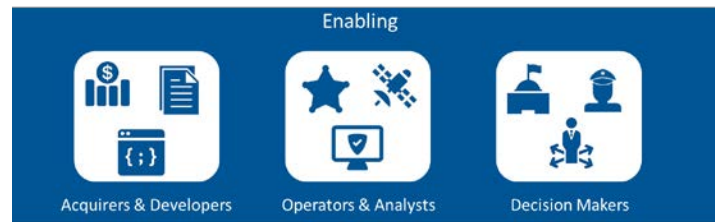
# Software Engineering Institute

A DoD R&D FFRDC operated by Carnegie Mellon University



## Mission

*To support the Nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring*



## NOTICE AND CONSENT



You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.

OK

Source: [DOD-CIO-CONSENT]

# Operating Model of Use Case

Provide value-add to existing security operations [EINSTEIN2-PIA] [EINSTEIN3A-PIA]

- Different tools may analyze the same source data
- Use of transparent middle-boxes for monitoring and mitigation
- Correlation occurs across “sites” and “protocol features”
- May be governed by Privacy Impact Assessments

Missions [GAO-16-294] [CJCSM-6510.B]

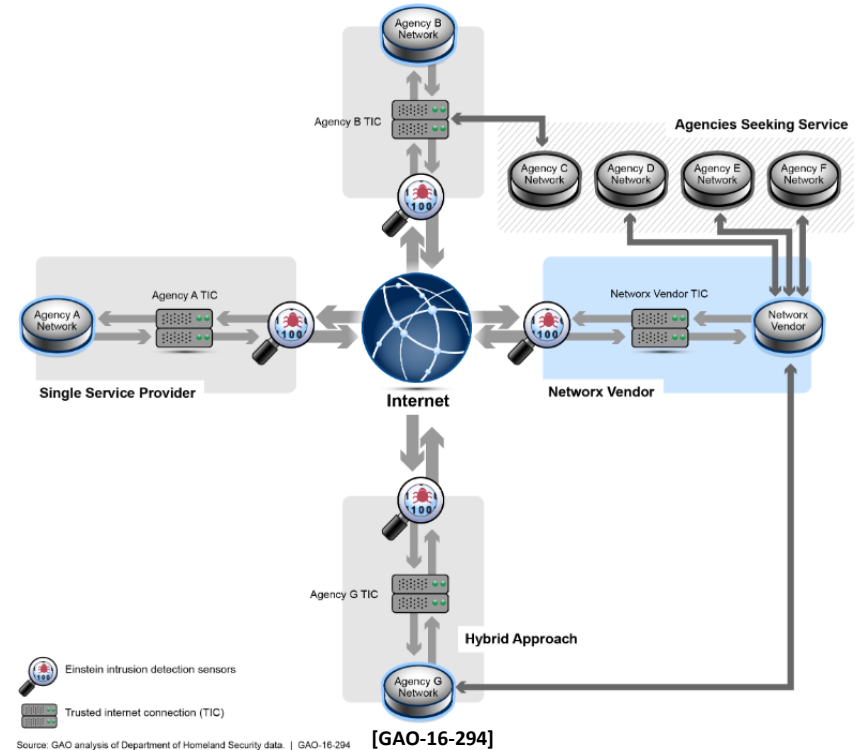
- Cross-organization visibility
- Targeted hunting and event mitigation
  - Data Loss Prevention
  - Intrusion Detection and Prevention
  - Incident Containment (Information Sharing)
- Incident Response



# Exemplar: National Cyber Security Protection System (EINSTEIN)

*EINSTEIN ... is to augment -- not replace or reduce -- the current computer network security practices of participating federal executive agencies. Participating agencies will continue to operate their own intrusion detection and prevention systems, perform network monitoring, and use other information security technologies. EINSTEIN ... enables the US-CERT to correlate activity across the entire federal enterprise.* [EINSTEIN2-PIA]

Figure 1: Interaction of Trusted Internet Connection and NCPS Intrusion Detection Sensors



# Coming Changes of Interest

## TLS v3 [PERVASIVE-CRYPTO]

- *Community Practice*: middle-boxes transparently terminating connections for inspection
- *IETF Background*: TLS (Transport Layer Security)
- *Future Work*: maintaining visibility with forward secrecy

## Encrypted DNS [PERVASIVE-CRYPTO]

- *Community Practice*: passive DNS monitoring in enterprise and at gateways
- *IETF Background*: DPRIVE (DNS PRIVate Exchange) and DOH (DNS Over HTTPS)
- *Future Work*: maintaining visibility

## MultiPath TCP [MULTIPATH-TCP]

- *Community Practice*: (asymmetric routing aside) inspection on single streams
- *IETF Background*: MPTCP (Multipath TCP)
- *Future Work*: evolving technology for multi-stream analysis

# Evolutions in Operating Model

## Temporary Loss Of Visibility

- Increased coordination between security operators

## Changes in workflow

- Acquiring features through alternative (non-network) sources
- PaaS and SaaS migration will put all security operators on equal footing
- Increased use of behavioral profiling

# References

**[CJCSM-6510.B]** Cyber Incident Handling Program. 2014.

<http://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897>

**[DOD-CIO-CONSENT]** Policy on Use of Department of Defense (DoD) Information Systems-Standard Consent Banner and User Agreement. 2008. <http://dodcio.defense.gov/Portals/0/Documents/DoDBanner-9May2008-ocr.pdf>

**[EINSTEIN2-PIA]** Privacy Impact Assessment of EINSTEIN 2. 2008

<https://www.dhs.gov/publication/dhsnppdpia-008-einstein-2>

**[EINSTEIN3A-PIA]** Privacy Impact Assessment of EINSTEIN 3 Accelerated. 2013.

<https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf>

**[GAO-16-294]** DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System. 2016. <https://www.gao.gov/products/GAO-16-294>

**[MULTIPATH-TCP]** Multipath TCP: Breaking today's network with tomorrow's protocols. 2014.

<https://www.blackhat.com/docs/us-14/materials/us-14-Pearce-Multipath-TCP-Breaking-Todays-Networks-With-Tomorrows-Protocols.pdf>

**[PERVASIVE-CRYPTO]** Effects of Pervasive Encryption on Operators. 2018. <https://datatracker.ietf.org/doc/draft-mm-wg-effect-encrypt/>