Carnegie Mellon University
Software Engineering Institute

Engineering for Cyber

Tim Chick

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

DM22-0158

Security Whac-A-Mole

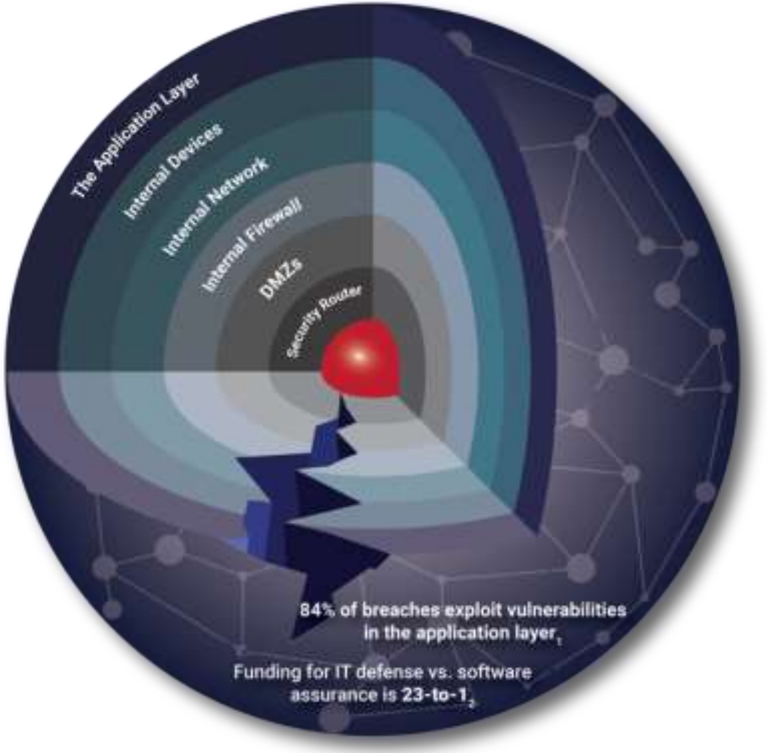
Winning in Features and Effectiveness, but Losing in Defensibility and Stability

In June of 2020 a generally successful DoD program completed an **8 week “Hardening the Software Factory” effort** in order to address **accumulated technical debt** and to address **insufficient security and operations** practices **due to the narrow focus on speed of delivery**.

These things occur, even in small relatively successful programs, when technical debt and insufficient security and operational practices are in place **due to lack of knowledge, experience, and reference material to fully design and execute an integrated DevSecOps strategy in which all stakeholder needs, including cybersecurity, are addressed.**

While playing Whac-A-Mole is inevitable, instead of missing the holes, or constantly hitting the same hole, the key is to fill in the holes.

Effective Security Requires a Holistic Approach


The Application Layer
Internal Devices
Internal Network
Internal Firewall
DMZs
Security Router
84% of breaches exploit vulnerabilities in the application layer[1]
Funding for IT defense vs. software assurance is 23-to-1[2]

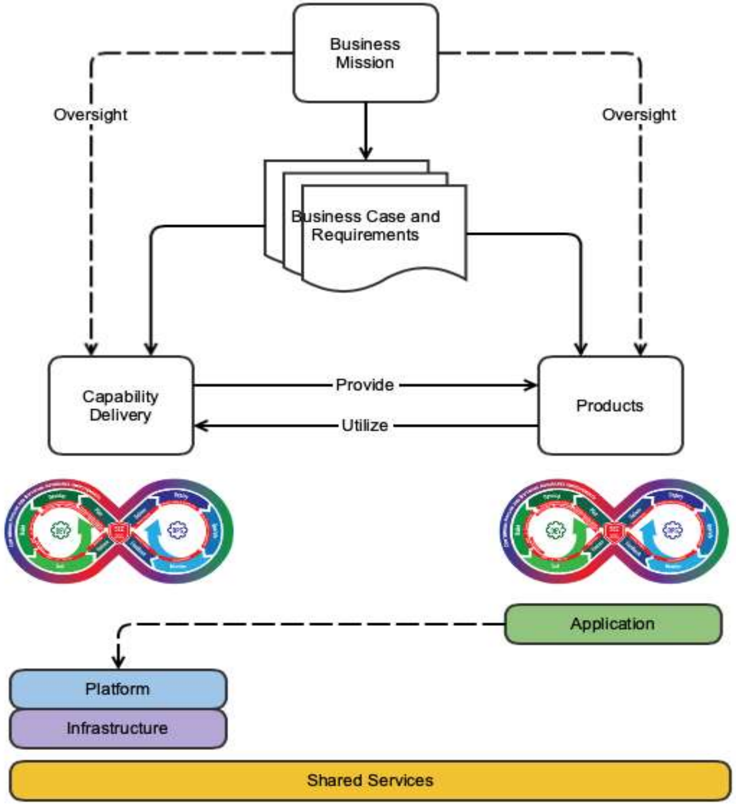
The Application Layer is the new perimeter exploited by 84% of breaches

Security must be Engineered into the Lifecycle of Applications changing the way we build and buy technology

- “76 percent of U.S. developers use no secure application program process”[4]
- “More than 40 percent of software developers globally say that security isn't a top priority for them”[4]
- 2017 less than 5% of DevOps initiatives have achieved the level of security automation required to be considered fully DevSecOps.[3]

1. Clark, Tim, *Most cyber Attacks Occur from this Common Vulnerability,* Forbes. 03-10-2015
2. Feiman, Joseph, *Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves,* Gartner. 09-25-2014. G00269825
3. *Horvath, Mark, Neil MacDonald, Ayal Tirosh: Integrating Security Into the DevSecOps Toolchain, Gartner. 11-16-2017. G00334264*
4. Microsoft[1] – http://visualstudiomagazine.com/articles/2013/07/16/majority-of-us-devs-dont-practice-secure-coding.aspx

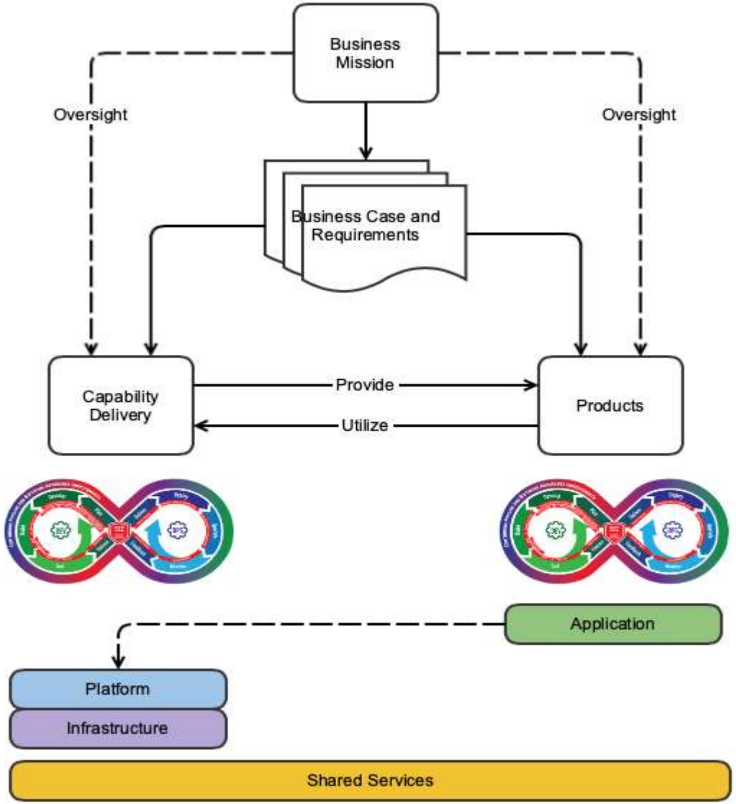
Challenge 1 for DevSecOps: connecting process, practice, & tools



Creation of the DevSecOps (DSO) pipeline for building the product is not static.

- Tools for process automation must work together and connect to the planned infrastructure
- Everything is software and all pieces must be maintained but responsibility will be shared across multiple organizations (Cloud for infrastructure, 3rd parties for tools and services, etc.)

Challenge 2 for DevSecOps: cybersecurity of pipeline and product



Business Mission

Oversight

Oversight

Business Case and Requirements

Capability Delivery

Provide

Utilize

Products

Application

Platform

Infrastructure

Shared Services

Managing and monitoring all of the various parts to ensure the product is built with sufficient cybersecurity and the pipeline is maintained to operate with sufficient cybersecurity is complex. Cybersecurity demands effective governance to address:

- What trust relations will be acceptable, and how will they be managed?
- What flow control and monitoring are in place to establish that the pipeline is working properly? Are these sufficient for the level of cybersecurity required?
- What compliance mandates are required? How are they addressed by the pipeline? Is this sufficient?

CERT - Engineering Focus

- Bringing **cyber to engineering** by helping organizations apply a holistic cybersecurity approach to software-intensive systems as they progress through the full system and software engineering lifecycles, defining and incorporating security strategies and automation into each phase to balance risk exposure with operational effectiveness
- Bringing **engineering to cyber** by helping organizations apply modern engineering practices to cyber domain systems and adopt emerging technologies at the rate needed to keep pace with evolving opportunities, threats, and risks

Key Expertise

Network sensing & traffic analysis

Systems supporting Security Operations

Risk Management Framework (RMF) and continuous Authority to Operate (cATO)

Model-based Systems Engineering (MBSE)

DevSecOps:

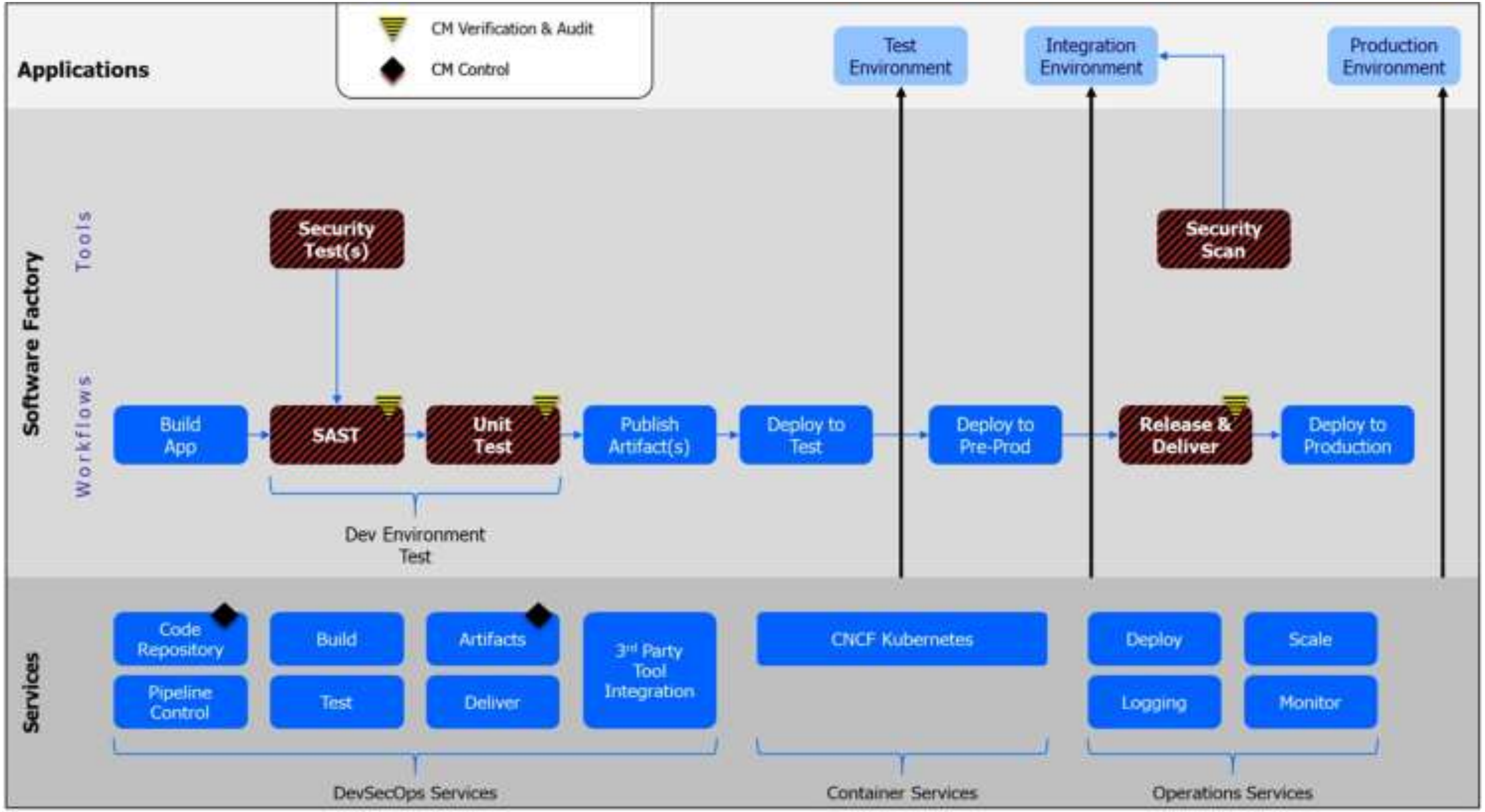
- Continuous Integration / Continuous Deployment
- Software Assurance Tool Integration
- Infrastructure-as-Code
- Containerization

Data Engineering:

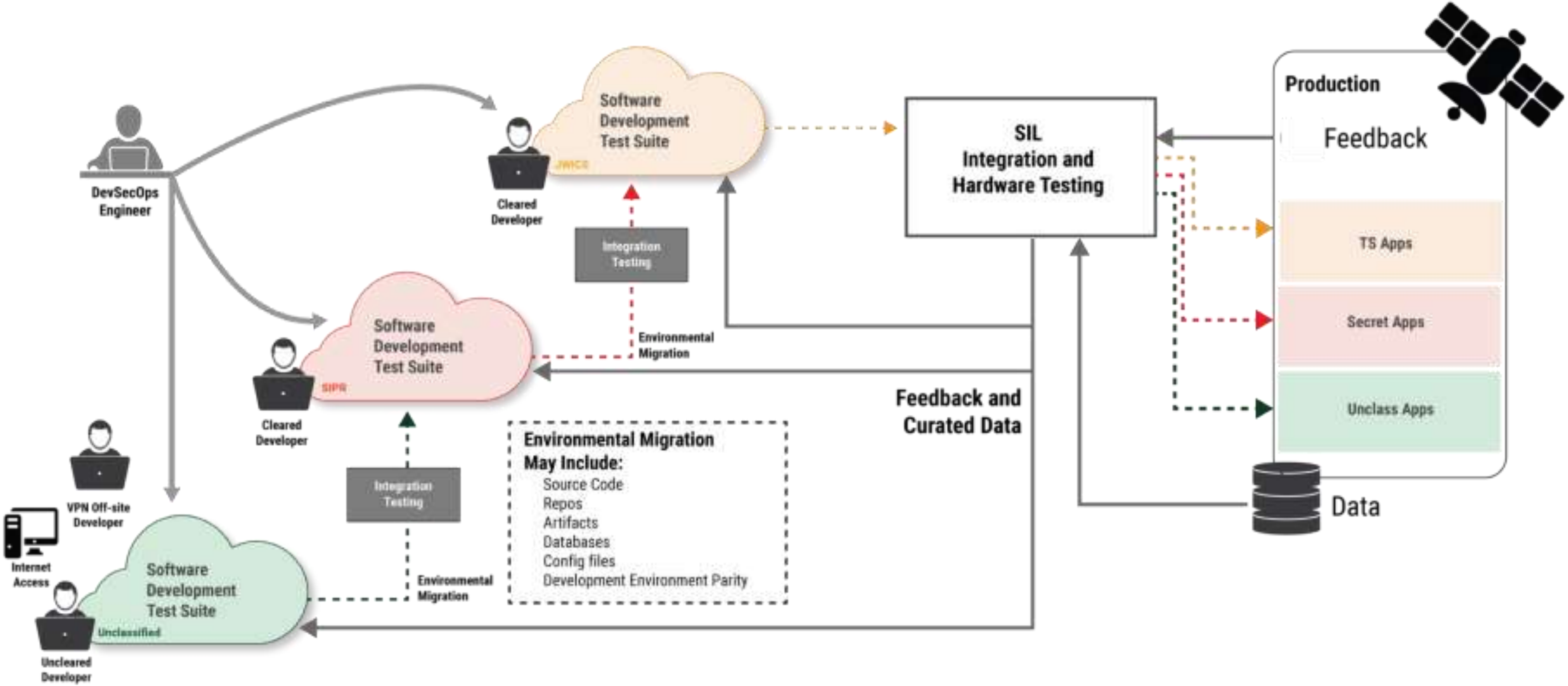
- Data processing & storage at scale
- Big Data (Spark, Hadoop, Elastic Stack)
- Automated data flow (Kafka, NiFi)

Cloud Services (Amazon Web Services, Azure)

Example Software Factory



Example Environmental Considerations



DevSecOps Engineer

Software Development Test Suite

JWICS

Cleared Developer

Integration Testing

Environmental Migration

Software Development Test Suite

SIPR

Cleared Developer

Integration Testing

Environmental Migration

VPN Off-site Developer

Internet Access

Software Development Test Suite

Unclassified

Uncleared Developer

SIL Integration and Hardware Testing

Feedback and Curated Data

Production

Feedback

TS Apps

Secret Apps

Unclass Apps

Data

Environmental Migration May Include:

- Source Code
- Repos
- Artifacts
- Databases
- Config files
- Development Environment Parity

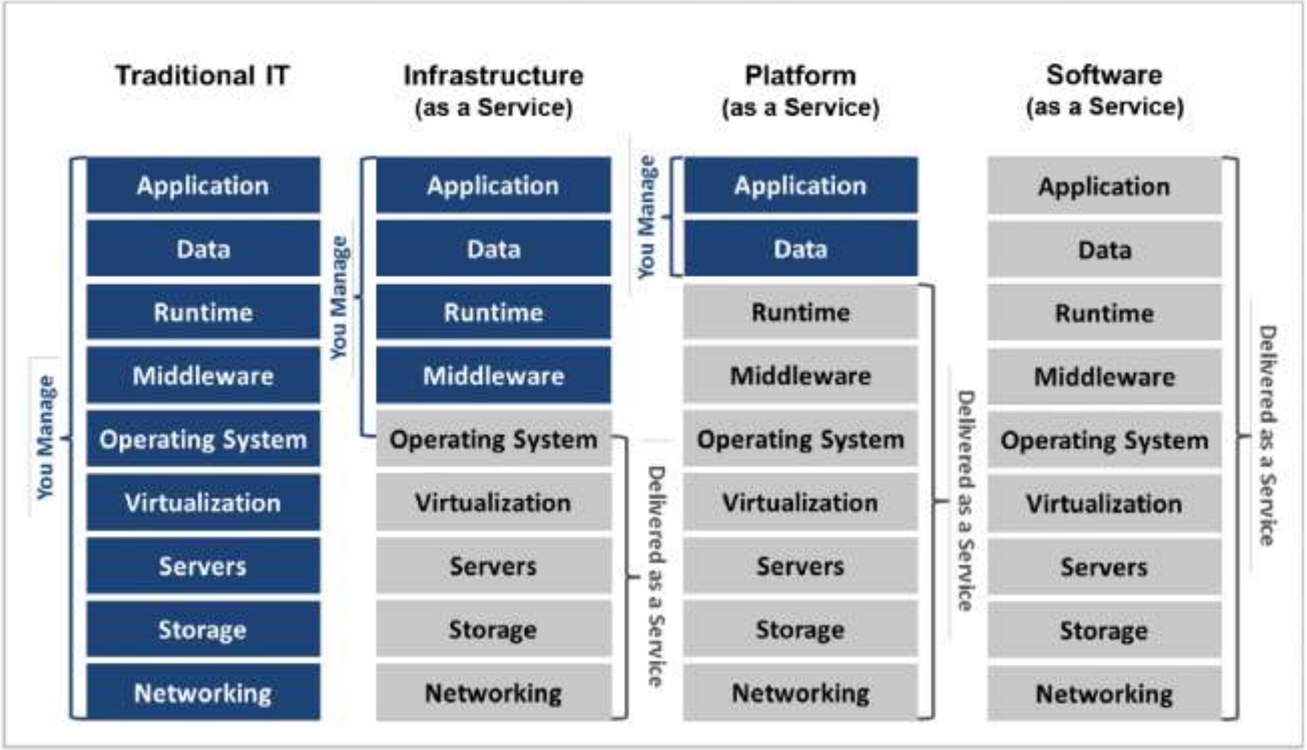
Cloud Concerns – Mission Suitability

- Cloud availability and performance baseline meet mission needs?
  - Commercial clouds generally guarantee only 99.95% uptime (varies service to service)
- Mission applications architected in a cloud-native, or minimally, cloud-compatible way?
- Do the costs of cloud align favorably with non-cloud options?
- Avoiding cloud service provider vendor lock-in
- If mission needs require special data handling (e.g., IL-4/5/6+) cloud options are more limited (both regions and resource types approved for use)

Cloud Concerns – Security

- Confidentiality
  - Communication between on-prem resources and cloud is properly protected from eavesdropping
  - Data within a cloud tenancy, at rest and in motion, is protected from eavesdropping from outside the cloud, another tenancy, or within the same tenancy from an unauthorized resource
- Integrity
  - Data transiting to/from the cloud is not tampered with
  - Data housed within the cloud tenancy cannot be altered without knowledge
- Availability
  - Cloud availability and performance meets or exceeds mission needs

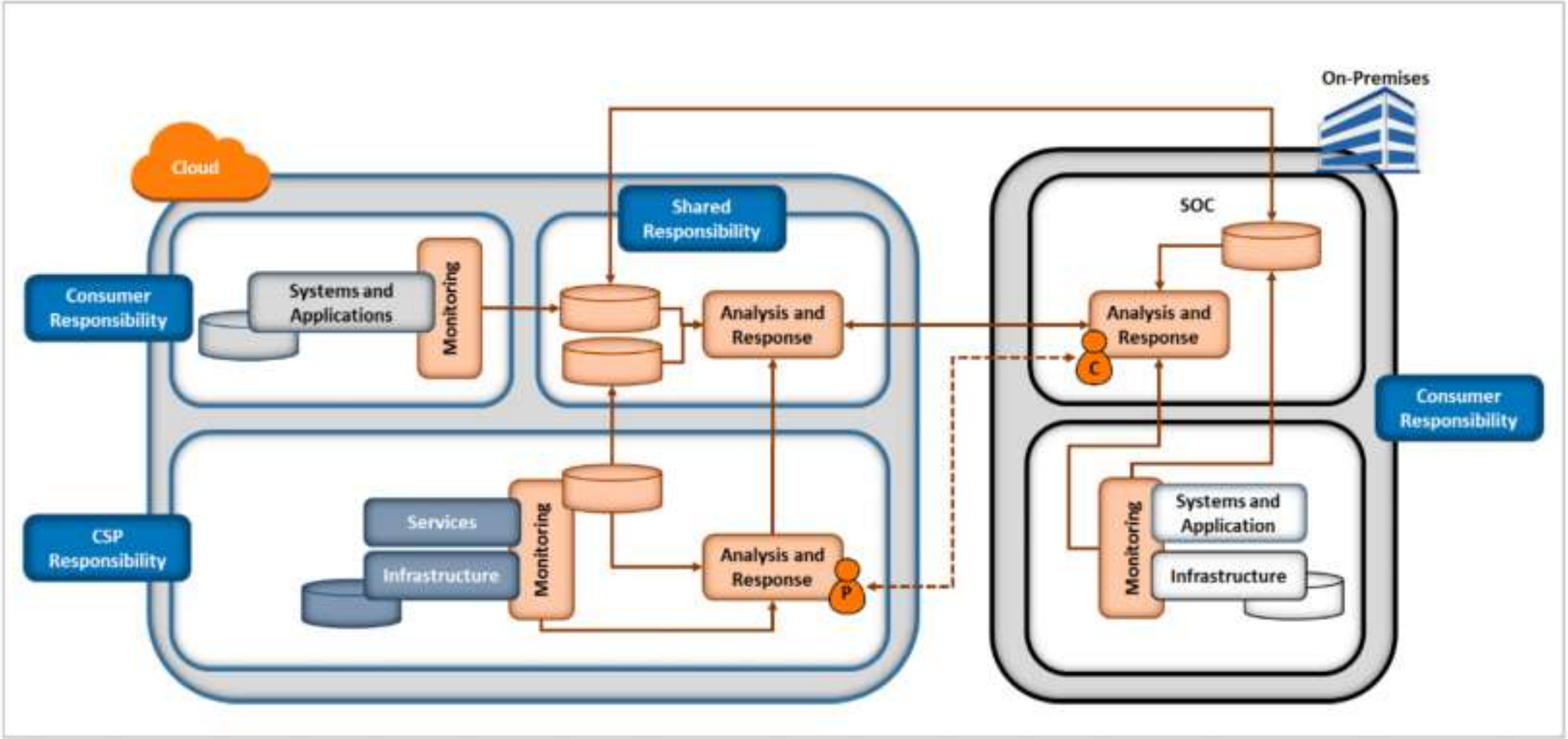
Shared Responsibilities



	Traditional IT		Infrastructure (as a Service)			Platform (as a Service)		Software (as a Service)	
You Manage	Application	You Manage	Application		You Manage	Application		Application	Delivered as a Service
	Data		Data			Data		Data	
	Runtime		Runtime			Runtime	Delivered as a Service	Runtime	
	Middleware		Middleware			Middleware		Middleware	
	Operating System		Operating System	Delivered as a Service		Operating System		Operating System	
	Virtualization		Virtualization			Virtualization		Virtualization	
	Servers		Servers			Servers		Servers	
	Storage		Storage			Storage		Storage	
	Networking		Networking			Networking		Networking	

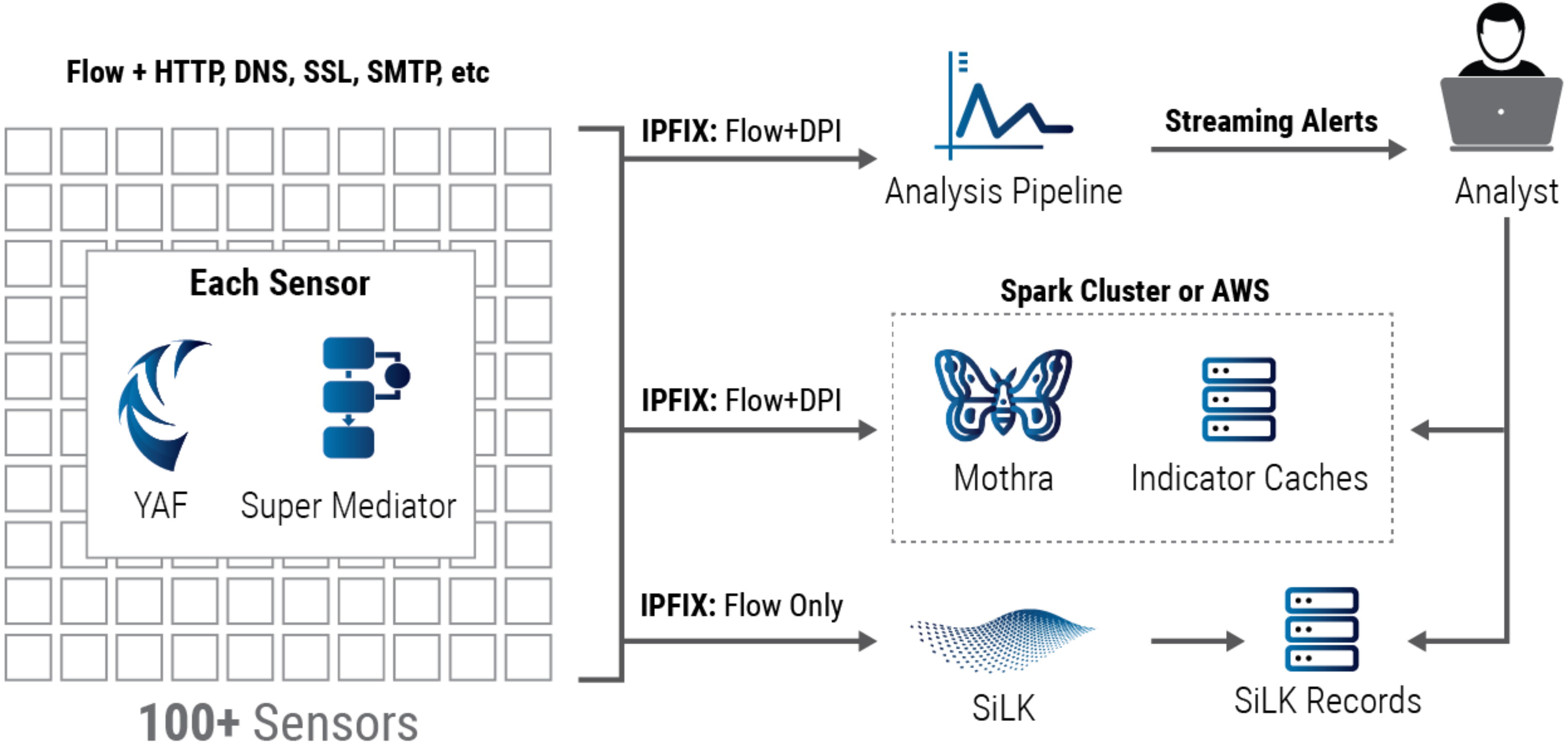
Source: Overview of Risks, Threat, and Vulnerabilities Faced by Agencies Moving to the Cloud, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=551354

Monitor and Defend



Source: Cloud Security Best Practices, Derived from Mission Thread Analysis, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=551466

SA’s NetSA Tool Suite Deployed at DHS in Einstein System



Tools have been open sourced to allow others to benefit from our research.

Network Data Collection Tools

End to end network collection suite

- Collection: Netflow plus deep packet inspection data
- Storage: Efficient cluster storage solution
- Analysis: Complete situational awareness
  - Streaming analytics
  - Data Labeling
  - Flow categorization

Customized data interfaces and analytic workflows

Advanced analytic platform

Data Integration and fusion

Einstein numbers:

- 100+ Billion flow records
- 1.2 Trillion Packets
- 958 Quadrillion Bytes (958 Terabytes)
- …per day
- Federate into a single ecosystem

The SEI product SiLK was the primary data source used by DHS Threat Hunting during the SolarWinds investigation.

https://tools.netsa.cert.org (Feb 2021-22)

- 26,828 web sessions
- 5,031 unique visits to download pages

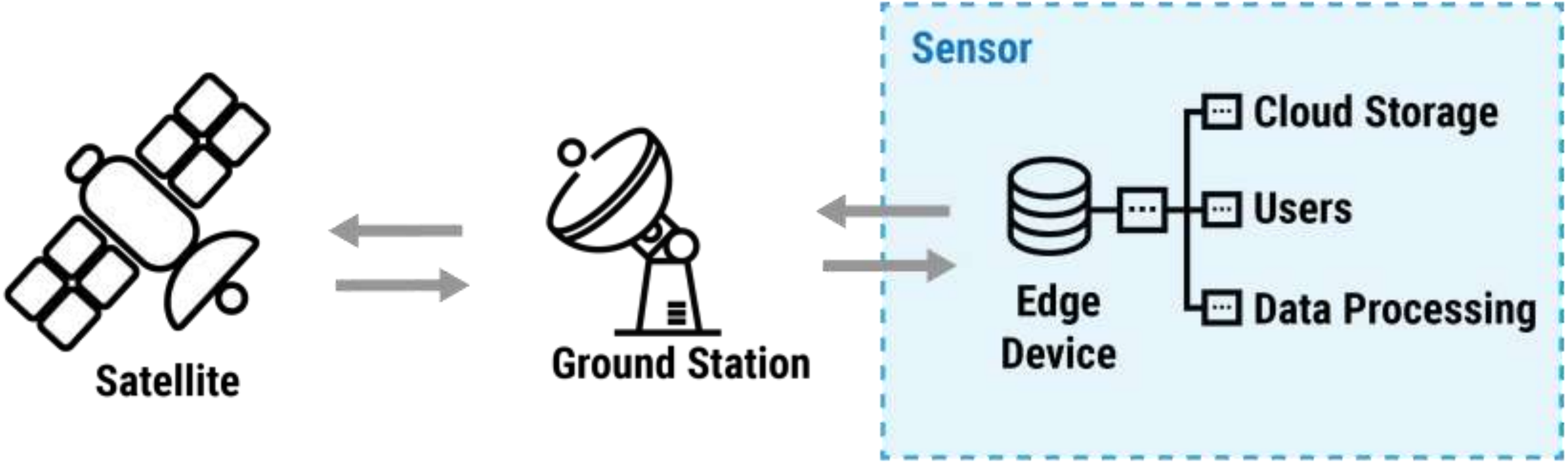
Potential NetSA Use Cases

Use Case	Question
Ensuring correct encryption always used	Are you sure the encrypted traffic is using the right protocol(s)?
Identify high byte counts to unapproved IP addresses	Do you know where all high-traffic connections are going?
Identify unexpected protocols used	Are you sure there are no unexpected protocols going across the connection?
Ensure all traffic has a mission case	Can you plot each connection to an explicit mission case?
Sync outgoing traffic with cloud logs	Can you compare outgoing flow logs to cloud logs to ensure they lineup to connections?

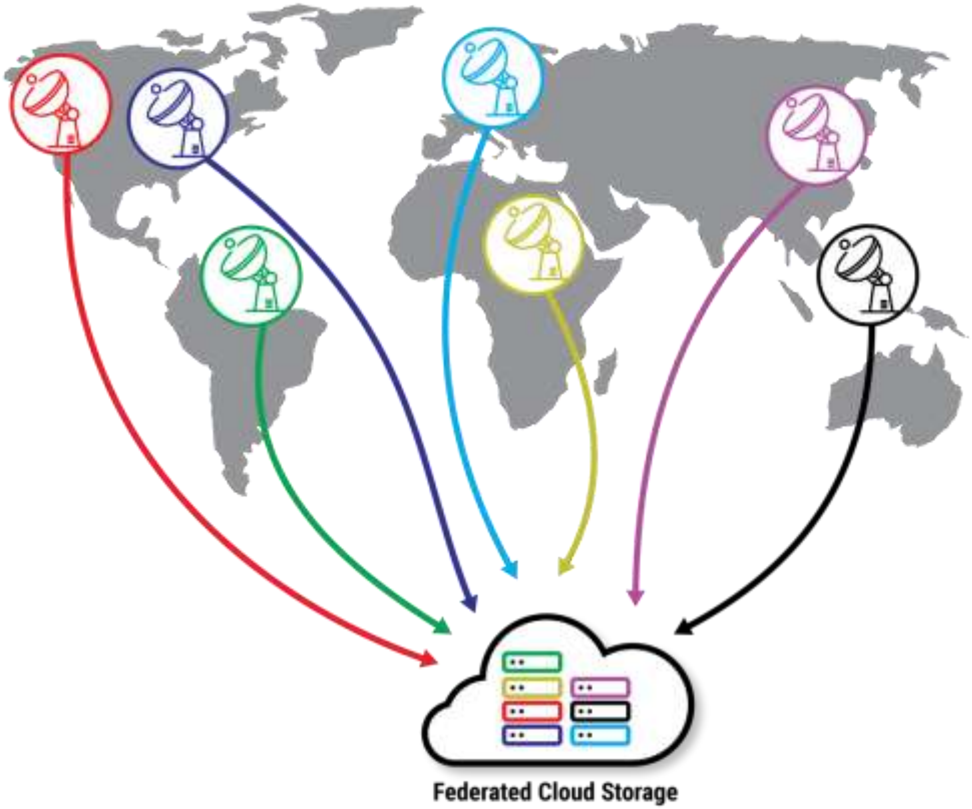
Features/Aspects:

- sensorID and Federation - Allows for global and targeted queries
- Custom network/sensor segmentation
- Custom Application Labels - Written by you or provided by the SEI
- Built for scale
- Own the data. Can access all of it. No third-party wall.
- Proactive automated approach reduces stress on the repo from periodic queries

Potential NASA Architecture - 1



Potential NASA Architecture - 2



Questions?

Through proper balance, programs should be able “to maintain a constant pace (i.e., play Topple) indefinitely” that results in a system that is:

- Trustworthy - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted
- Predictable - When executed, software functions as intended and only as intended

Contact Information

Tim Chick - tchick@sei.cmu.edu

http://www.sei.cmu.edu/

Backup

DevSecOps Challenges

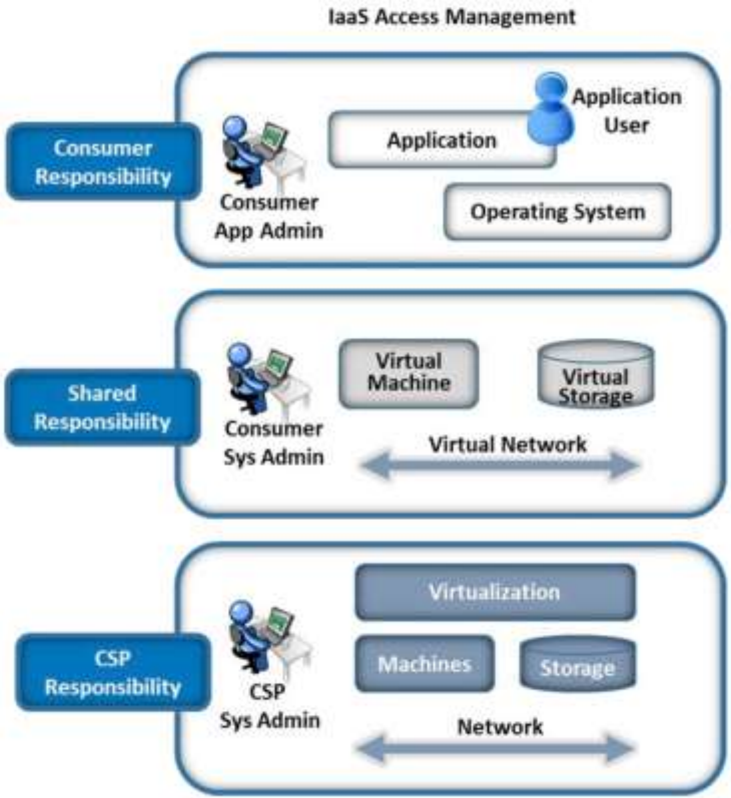
- ***Emerging technology challenges:*** Incorporation of AI/ML models built, trained, tested, and validated within the pipeline
- ***Hardware in the Loop challenges:*** Application to Large Highly Regulated, Cyberphysical Systems of Systems
- ***Governance and collaboration challenges:*** Evolution of oversight, evaluation, and collaboration practices for nimble delivery of value
- ***Architectural challenges:*** Compatible architecture that supports iterative and incremental development
- ***Digital Engineering(DE) and Model Based System Engineering(MBSE) adoption challenges:*** Incorporation of DE and MBSE approach with DevSecOps

Establishing Dev{*} Pipeline

- To enable the fielding of capabilities at the speed of relevance, SEI researches and transitions technologies that provide a pipeline capable of delivering with speed, quality, focus, and collaboration.

- Focusing on realizing pipelines that meet:
  - Emerging technology challenges: Incorporation of AI/ML models built, trained, tested, and validated within the pipeline
  - Hardware in the Loop challenges: Application to Large Highly Regulated, Cyberphysical Systems of Systems
  - Governance and collaboration challenges: Evolution of oversight, evaluation, and collaboration practices for nimble delivery of value

Assess Management and Shared Responsibility



Source: Cloud Security Best Practices, Derived from Mission Thread Analysis, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=551466