# Cyber Resiliency Against Supply Chain Attacks

Paul Bicknell
William Heinbockel
Ellen Laderman
Gloria Serrao

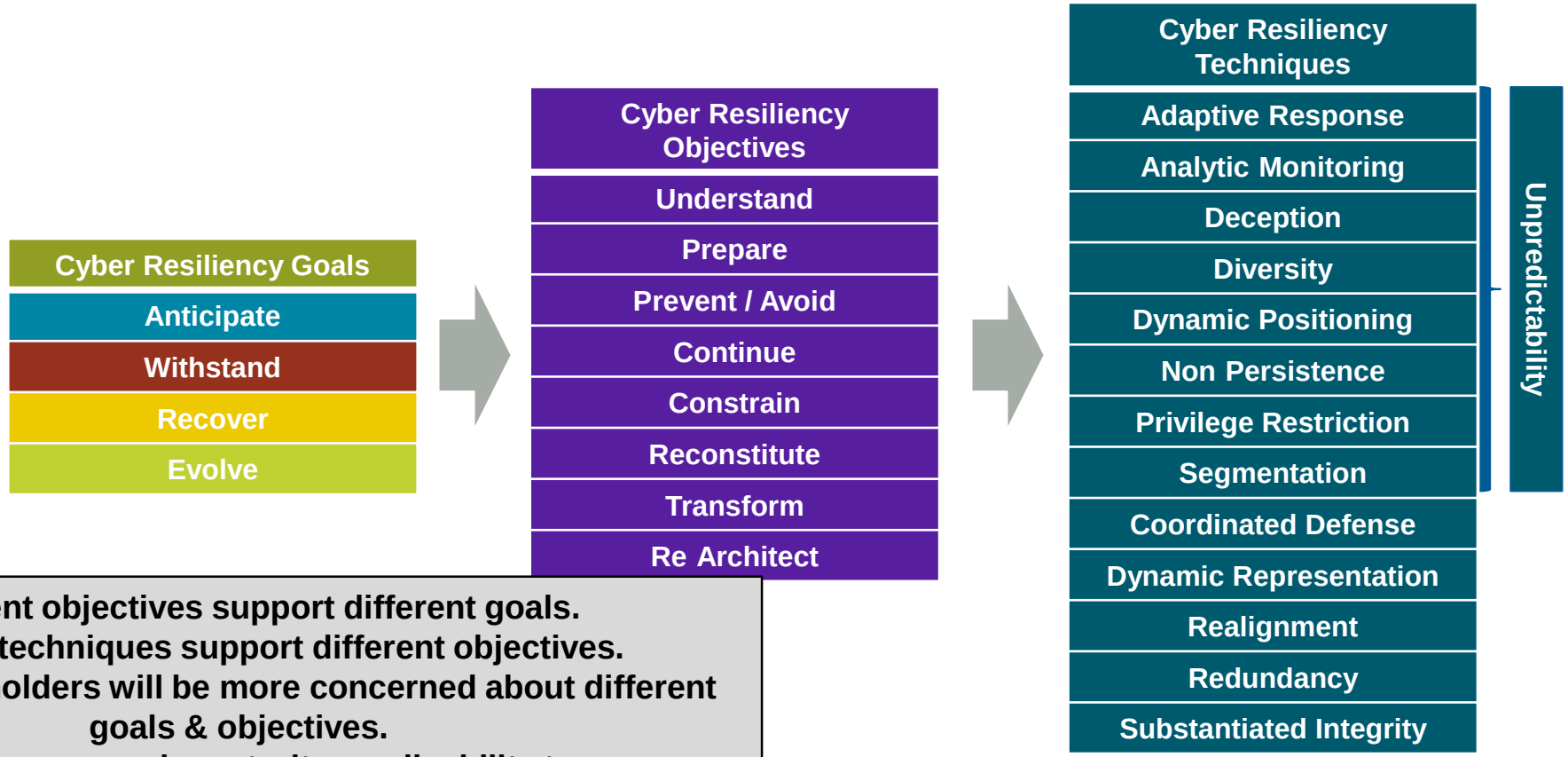
# Task Overview

- **Goal 1: Ensure Operational Mission Assurance despite supply chain threats**
  - Mission and supporting cyber resources  are able to: anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises caused by supply chain attacks
    - Builds on previously defined supply chain attacks and provides security engineering guidance
    - **FOR** applying Cyber Resiliency Mitigations (techniques) across the entire acquisition life cycle
    - **WITH** emphasis on adversarial threat and mitigating successful attacks on an operational environment
- **Goal 2: Provenance (origin and chain of custody in supply chain)**
  - Survey existence provenance requirements and solutions
  - Provide guidance to Integrators and Acquisition Support



MITRE

# MITRE's Cyber Resiliency Engineering Framework: Quick Review




**Different objectives support different goals.**
**Different techniques support different objectives.**
**Different stakeholders will be more concerned about different goals & objectives.**
**Techniques vary in maturity, applicability to architectural layers, and suitability to operational environments – no system can (or should) apply them all.**

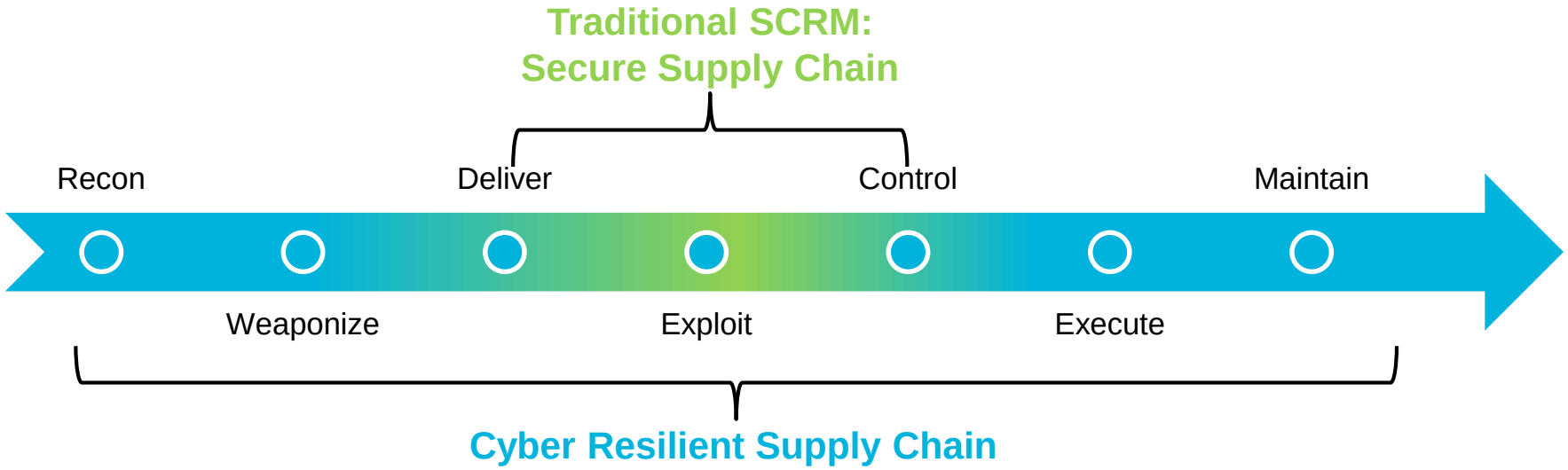
Approved for Public Release;
Distribution Unlimited. Case Number 17-3169



MITRE

# Focus & Cyber Attack Lifecycle

- **Traditional SCRM and acquisition requirements focus on cybersecurity and preventing adversary exploit and delivery**
  - DoDI 5000.02; NLCC; NIST SP 800-53, 800-161
- **Our effort complements SCRM by increasing cyber resiliency against the whole cyber attack lifecycle**






MITRE

# Goal 1
# Resiliency and Supply Chain Attacks

# … can attack the entire Acquisition Lifecycle

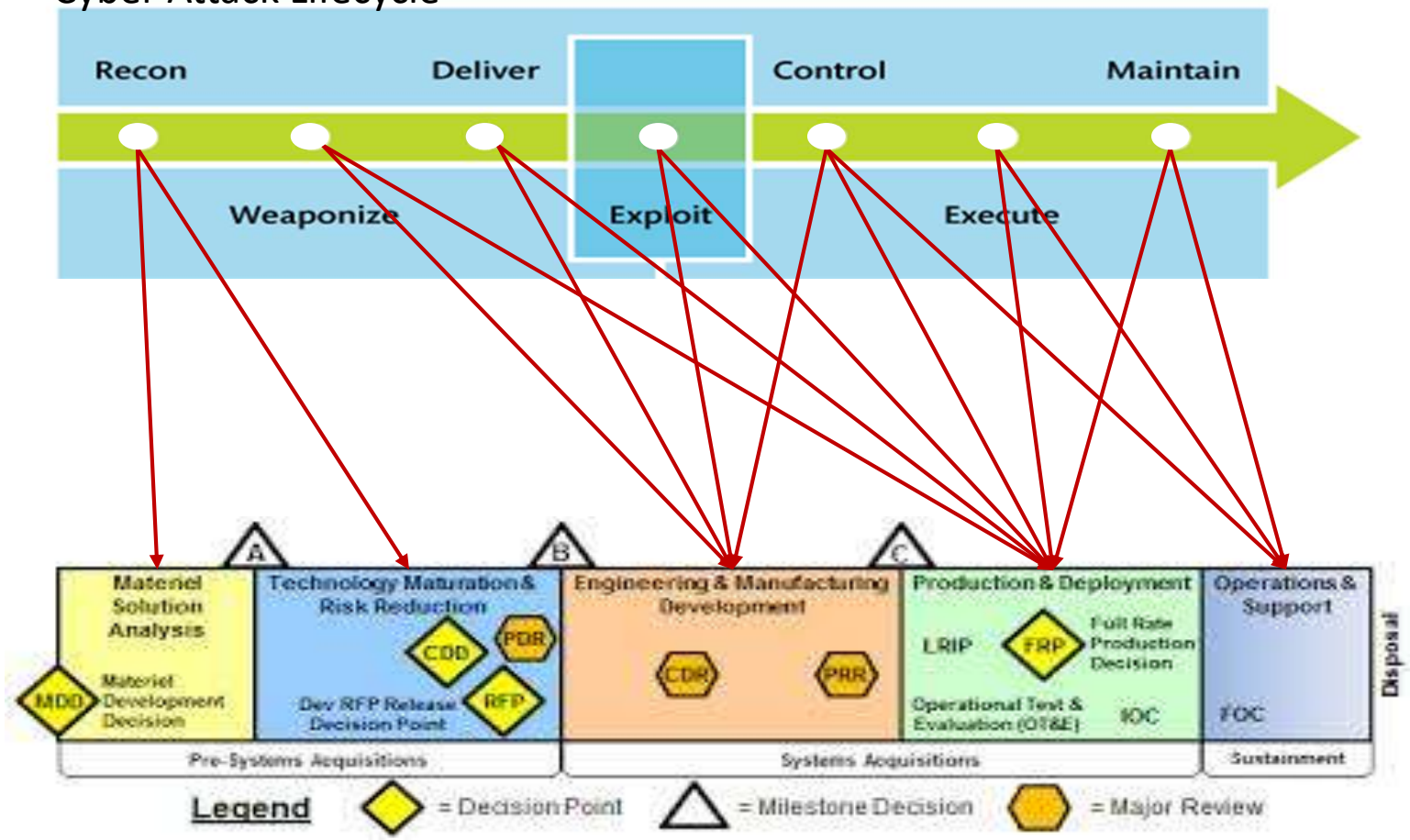
**Adversary Goals:**

- Acquire information
- Develop tools
- Deliver attack
- Initiate exploit
- Control attack
- Execute main attack
- Maintain presence

**Defender Goals (relative to Operations and Support):**

- Reduce attacks
- Limit attacks that can't be eliminated
- Gain and share information about attacks

Cyber Attack Lifecycle




Acquisition Lifecycle

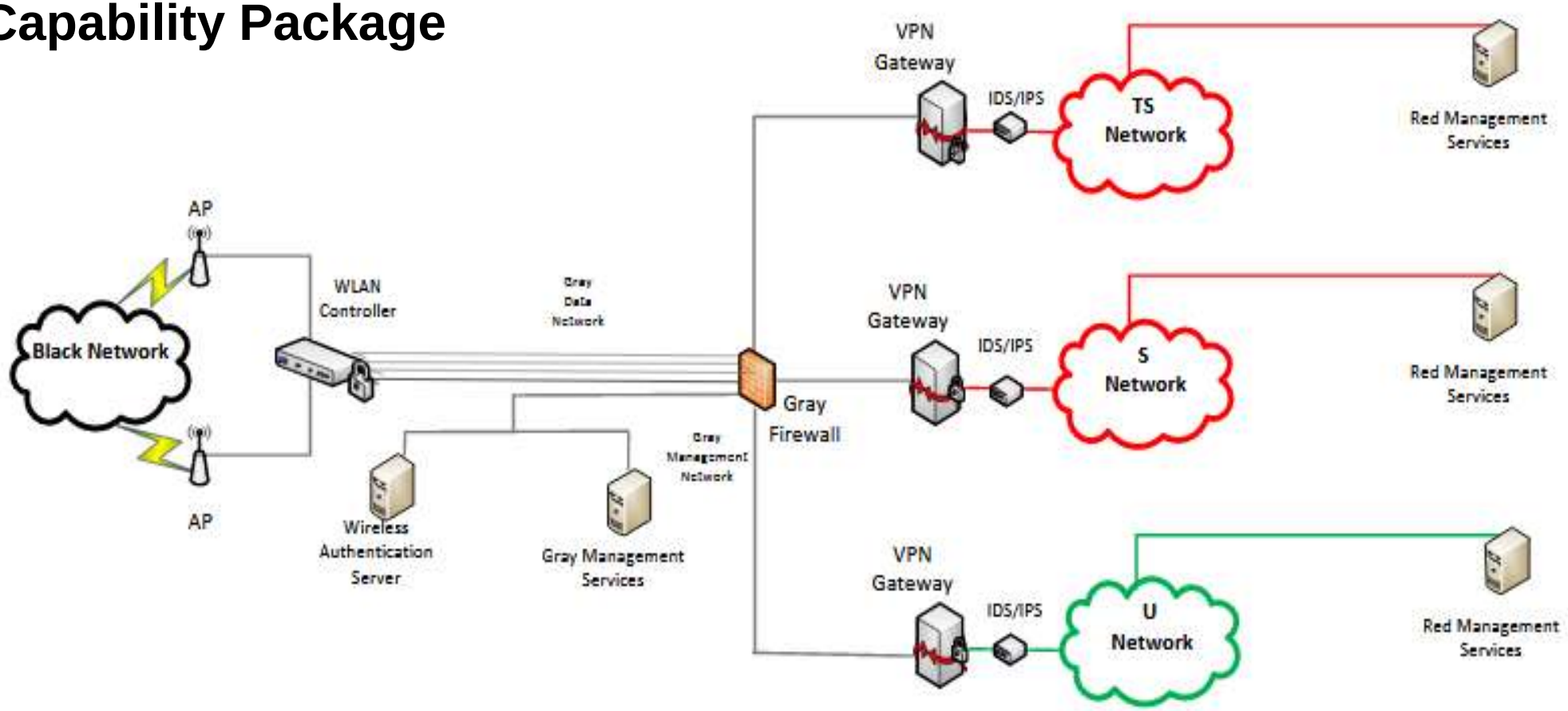




MITRE

# Example: Adversary Attack on WLAN Supply Chain

- **Architecture based on Campus Wireless Local Area Network (WLAN) CSfC Capability Package**



# Adversaries have multiple opportunities to attack acquisitions

- **MSA/TMRR**
  - Modify WLAN ICD/CDD, requirements (e.g., KPPs, KSAs)
  - Reconnoiter potential capabilities, risk decisions
  - Influence acquisition strategy
- **EMD**
  - Modify system, hardware designs
  - Implant, modify code
  - Modify technical, operational requirements
  - Impair validity tests
- **P&D**
  - Implant, modify code
  - Introduce counterfeit components
- **O&S**
  - Implant, modify code
  - Modify configurations

**Mission Impacts**

- Weaker Security
- Reduced Robustness
- Degraded WLAN Service
- Loss of User Confidence
- Increased Data Exfiltration Risk

Approved for Public Release;
Distribution Unlimited. Case Number 17-3169

# Most Effective Phases to Apply Cyber Resiliency

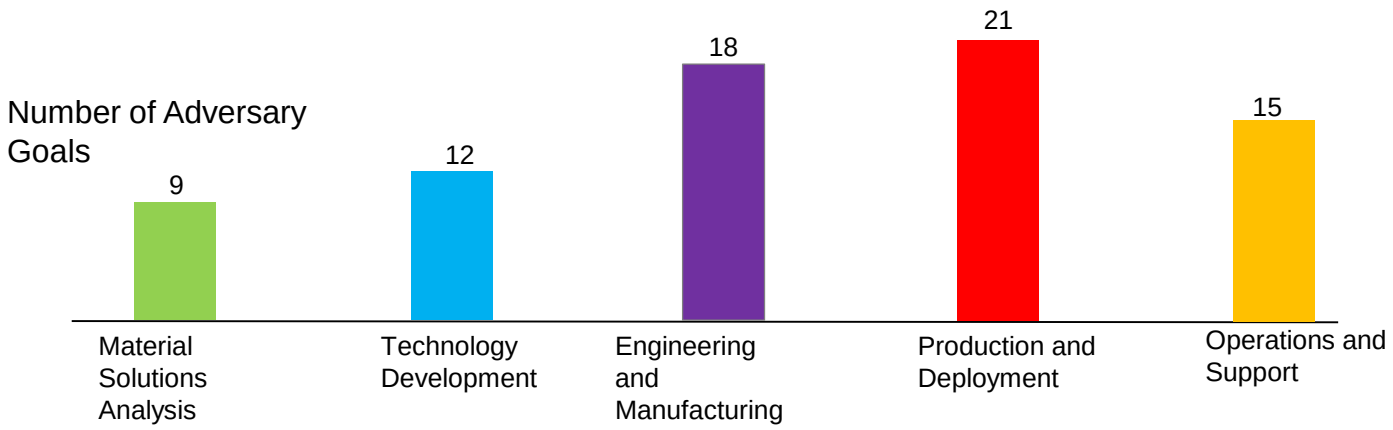
- ***Production & Deployment*** **phase is associated with the most adversary Goals**
- ***Engineering & Manufacturing Development and Production and Deployment*** **phases**
  - Product Development and Definition
  - “biggest bang for the buck”
  - Non-operational environments → more flexibility in mitigation deployment
  - Best opportunity for defenders to apply resiliency techniques and approaches
  - Largest impact to adversary goals
  - Best chance to achieve defender goals
- **Supply chain threat mitigations in O&S are a double-edged sword: mitigations enhance operational resilience, but can add additional complexity**

# Non Persistence throughout the Acquisition Lifecycle (1of 2)

| Acquisition Lifecycle | Resiliency Mitigations | Adversary Goals (per the CAL) | | | | | | | Defender Goals in O&S | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Acquire Info | Develop tools | Deliver Attack | Initial Exploit | Controlling attack | Executing Attack | Maintain Presence | Reduce attacks | Limit attack | Gain/Share Info | Recover |
| Materiel Solutions Analysis | Non-Persistent Information – Reduce availability of information about system needs and development | x | | | | | | | x | x | | |
| | Non-Persistent Services – Reduce the chance the adversary has corrupted services in the environment to gain information | x | | | | | | | x | x | | |
| | Non-Persistent Connectivity – reduce the means to get the information about system needs and developments | x | | | | | | | x | x | | |
| Technology Development | Non-Persistent Information – limit the adversary's ability to gain information by limiting the time the information is available | **x** | | | | | | | **x** | **x** | | **x** |
| | Non-Persistent Services – limit the amount of time the adversary can exploit a service | **x** | | | | | | | **x** | **x** | | **x** |
| | Non-Persistent Connectivity – limit the amount of time paths into the environment are available | **x** | | | | | | | **x** | **x** | | **x** |
| Engineering and Manufacturing | Non-Persistent Information – limit the adversary's ability to deliver an attack, decrease the probability of the initial exploit being successful and reduce the adversary's ability to control malware by limiting the time information is available | **x** | | **x** | **x** | **x** | | | **x** | **x** | | |
| | Non-Persistent Services – limit the adversary's ability to deliver an attack, decrease the probability of the initial exploit being successful and reduce the adversary's ability to control malware by limiting the amount of time the adversary can exploit a service | **x** | | **x** | **x** | **x** | | | **x** | **x** | | |
| | Non-Persistent Connectivity – limit the adversary's ability to deliver an attack, decrease the probability of the initial exploit being successful and reduce the adversary's ability to control malware by limiting the amount of time paths into the environment are available | **x** | | **x** | **x** | **x** | | | **x** | **x** | | |

# Non Persistence throughout the Acquisition Lifecycle (2 of 2)

| Acquisition Lifecycle | Resiliency Mitigations | Adversary Goals (per the CAL) | | | | | | | Defender Goals in O&S | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Acquire Info | Develop tools | Deliver Attack | Initial Exploit | Controlling attack | Executing Attack | Maintain Presence | Reduce attacks | Limit attack | Gain/Share Info | Recover |
| Production and Deployment | Non-Persistent Information – limit the adversary's presence from delivery through maintenance by limiting the time information is available | | | x | x | x | x | x | x | x | | |
| | Non-Persistent Services – limit the adversary's presence from delivery through maintenance by limiting the time the adversary can exploit a service | | | x | x | x | x | x | x | x | | |
| | Non-Persistent Connectivity – limit the adversary's presence from delivery through maintenance by limiting the time paths into the environment are available | | | x | x | x | x | x | x | x | | |
| Operations and support | Non-Persistent Information – limit the adversary's presence throughout the CAL by limiting the time information is available | | | | | x | x | x | x | x | | x |
| | Non-Persistent Services – limit the adversary's presence throughout the CAL by limiting the time the adversary can exploit a service | | | | | x | x | x | x | x | | |
| | Non-Persistent Connectivity – – limit the adversary's presence throughout the CAL by limiting the time paths into the environment are available | | | | | x | x | x | | x | | |



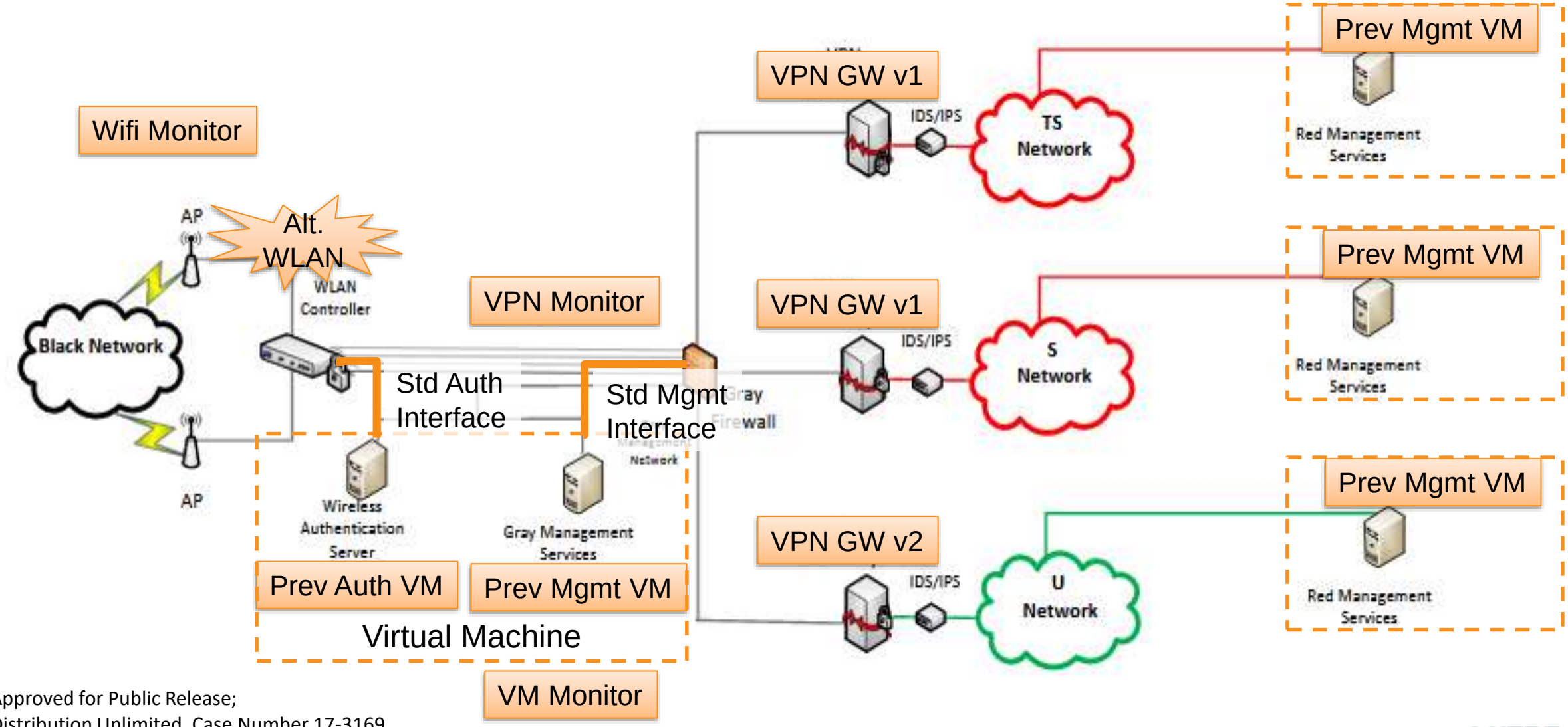



MITRE

# Guidance for Applying Cyber Resiliency

- **Identify effective mitigations by "thinking backwards"**
  - Start with the "as-is" or "to-be" mission system
  - Working in reverse through the Acquisitions Lifecycle phases
  - For each phase, answer the following questions
- **Q1 What are the likely impacts of a successful supply chain attack to the identified critical assets?**
- **Q2 How can you tell if the supply chain is attacked or compromised?**
  - Authenticity, verification testing
  - Baseline and trend monitoring can identify counterfeit and potential compromise
- **Q3 How will you recover from the attack or compromise?**
  - The earlier in the acquisition the attack took place, the harder it is to recover
  - Agile, segmented design and virtualization allows for quick replacement
  - Supporting technology standards allows for easier product replacement

# Mitigating WLAN CP Supply Chain Threats








MITRE

# Applying Resilience Against Supply Chain Threats

## Resilient Acquisitions

- Use access-controlled “gold master” images for designs, documents, and software
- Limit the connectivity to, duration of, and information stored on user’s machines
- Design around industry standards
- Design and build in ways for verification testing
- Compartmentalize acquisitions insight and knowledge
- Substantiate provenance with each transfer of stewardship

## Resilient Operations

- Validation & verification testing of updates and new components
- Enable efficient rollback to previous versions: swappable WLAN Controllers, Versioned VMs
- Maintain list of alternate supply chain products and providers: WLAN Controller, VPN Gateways
- Monitor behavior: wireless RF, VPN, VM
- Segment management and data channels to minimize visibility
- Consider alternative ways to prevent/detect instead of patching vulnerabilities (e.g., CDS, IDS)

# Goal 1 – Initial Findings

- **During operations, Cyber Attacks and Supply Chain attacks are not easily differentiated. However:**
  - For Supply Chain attacks pre-exploit actions (weaponize and deliver) happen in early acquisition phases
  - This early established presence is difficult to detect at perimeter
- **Resiliency mitigations <u>can be</u> applied for all assets across all acquisition phases**
- **Best when "built in" early in acquisition**
- **Best Phases are Engineering and Manufacturing Development and Production and Deployment**
  - More Flexibility
  - Less Complexity
    - As compared to O&S
  - Provenance and integrity validation can be designed in
  - Most mitigations in these phases also mitigate supply chain threats during O&S

# Goal 2
# Supply Chain Provenance

# Goal 2 – Achieving Provenance in the Supply Chain

- **Provenance substantiates integrity of the supply chain**
- **Minimize risks while moving through the supply chain**
  - Malicious insertions
  - Component substitutions (modified or counterfeit)
- **Achievable through technical and procedural methods**
  - Technical methods track custody and can prevent/interfere with physical or logical modifications
  - Procedural methods monitor and enforce handling and delivery practices

# Substantiated Integrity – Provenance Tracking

**Goal: Establish a verifiable history of component "ownership"**

- Maintain a "chain of custody" of stewardship or possession
- Track and audit modifications: who, what, when

1. **Identify interface points along the supply chain**
   - Developer → solution integrator → production facility → end user
2. **Require appropriate technical/procedural methods for each component involved in exchange**
3. **Record stewardship with each exchange**
4. **Record/categorize modifications that have taken place at each point along the supply chain**
   - Include "chain of custody" record as part of the exchange
   - Provide means of confirming and verifying provenance record at each exchange

# Provenance Initial Findings

- **Documented criteria and existing solutions for critical components**
  - Overall Provenance Program is necessary
  - Provenance Solutions will be required for specific components
- **Identified variety of available technologies and methods**
  - Many only provide a portion of needed capabilities
- **Challenges**
  - Few technologies are useful through the entire lifecycle
  - Combining information from different technologies/methods appears difficult

# Back Up Slides

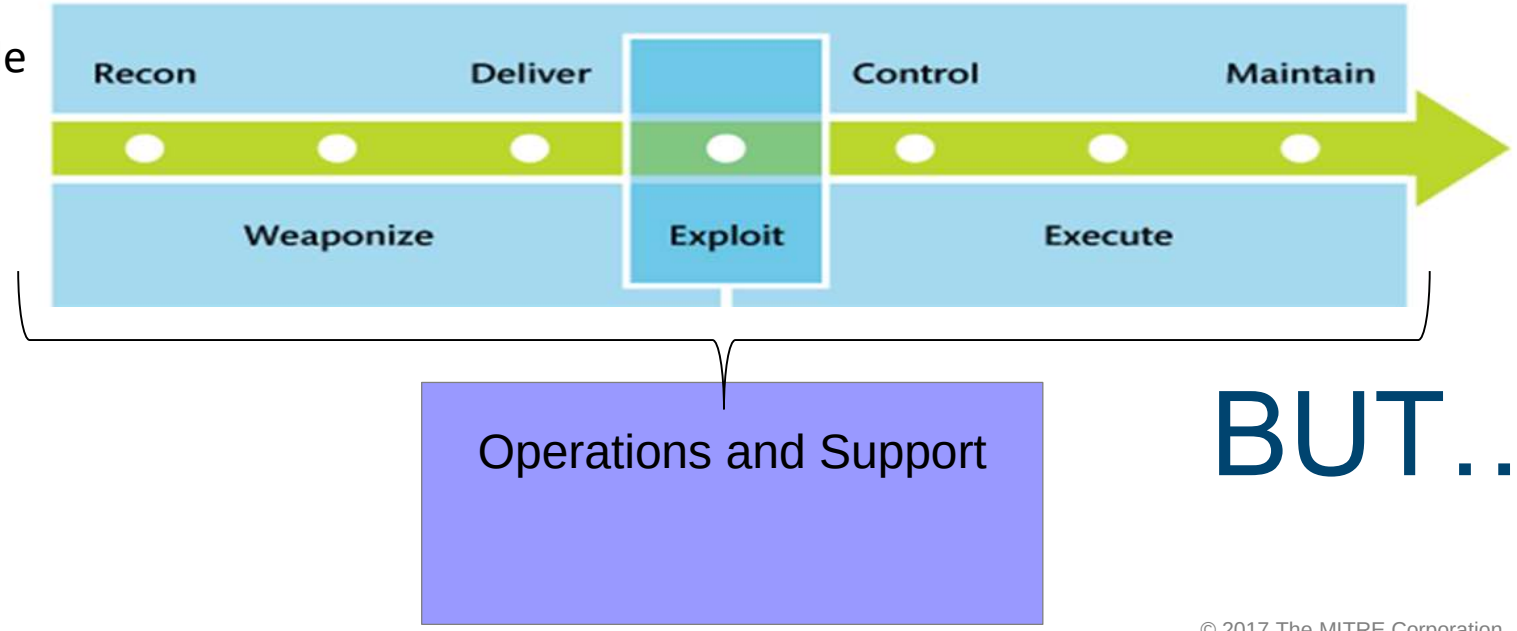
# Provenance Methods

- **Example Technical Methods**
  - Physical: Secure Packaging, tamper-evident seals, locks, etc.
  - Hardware: Root of Trust Technologies (TPM), DARPA Shield, device identifiers
  - Firmware, Software, Documents: Cryptographic signing, Blockchains
- **Example Procedural Methods**
  - Component naming schemes
  - Secure delivery specifications and procedures

# Adversaries want to impact Operations

- Violate Confidentiality (intercept)
- Destroy Integrity (fabricate, modification)
- Reduce Availability (degrade, interrupt),
- Use resources for illegitimate purposes (unauthorized use)

Cyber Attack Lifecycle




BUT….



MITRE

# WLAN Assets have multiple supply chain attack vectors

| | WLAN Asset | HW | FW | SW | Docs |
|---|---|---|---|---|---|
| *Rqmts* | ICD/CDD, KPPs/KSAs | | | | X |
| | System, Software/Hardware Design | | | | X |
| | Operational & Derived Requirements | | | | X |
| *Technology* | Wireless Access Points | X | X | | |
| | WLAN Controller | X | X | | *Config |
| | Authentication Server | X | X | X | *Config |
| | Management Services | X | X | X | *Config |
| | Firewall | X | X | | *Config |
| | VPN Gateways | X | X | | *Config |
| | IDS/IPS | X | X | X | *Config |

# Provenance Effort Status

- **Current Activities**
  - Identify suitable technologies and methods
  - Document requirements and existing solutions for critical components
  - Create starting point for integrators and end users
    - Contribute to the establishment of a provenance-assuring program throughout the component lifecycle
- **Challenges**
  - Few technologies are useful through the entire lifecycle
  - Combining information from different technologies/methods is a difficult problem

# Non-Persistence (Information, Services, Connectivity)

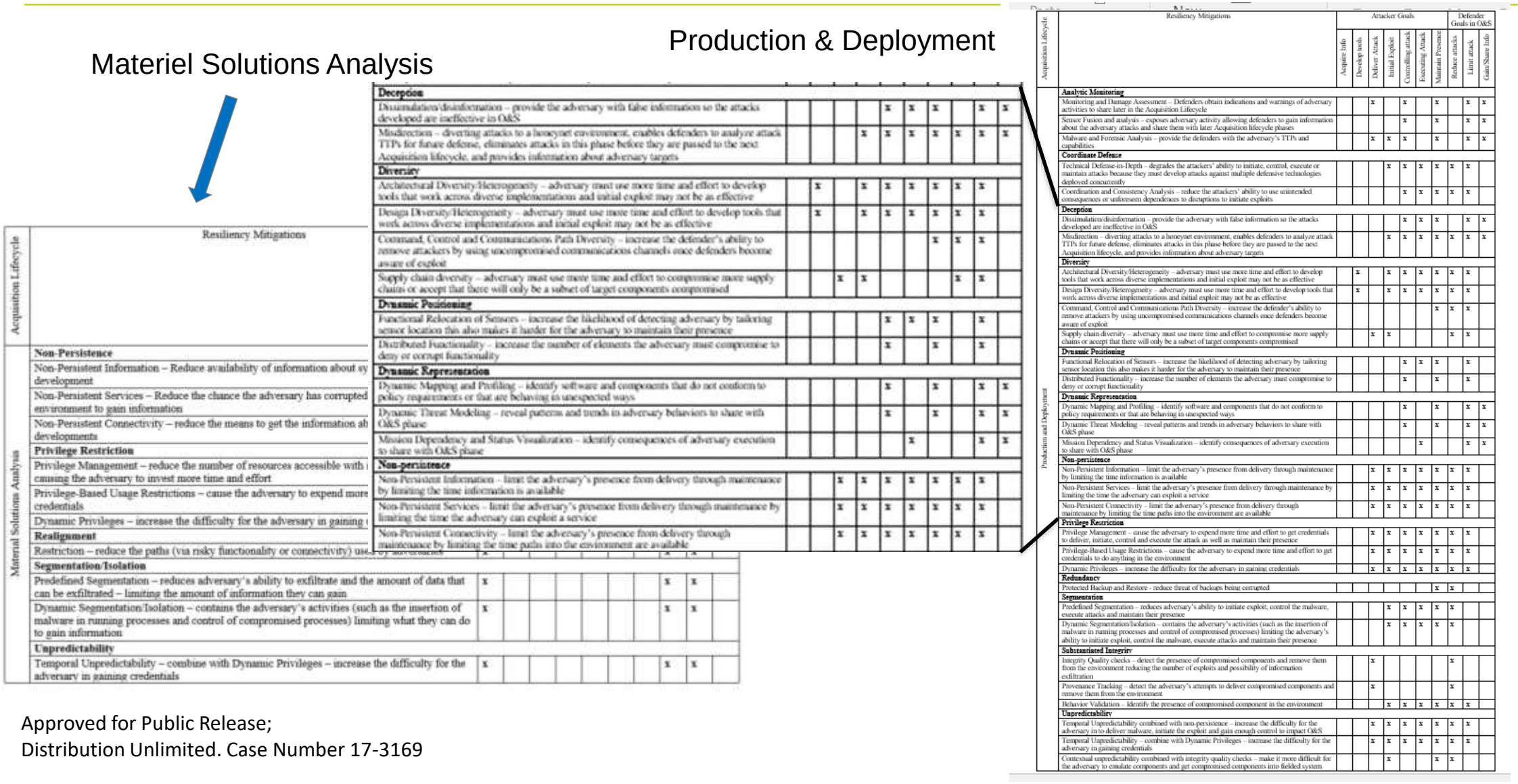
- ***Material Solutions Analysis*** **Phase: makes it more difficult for the adversary to acquire information**
- ***Production & Deployment*** **Phase: limits the paths for the adversary to get into the environment hampering their efforts and delivering, initiating controlling, executing or maintaining their attacks.**
- ***Operations & Support*** **Phase: limits the time and methods for the adversary to control execute and maintain their attacks**
- **→ Using Non-Persistence in all three phases has the effect of reducing the number and effectiveness of attacks in O&S**
- **→ Using this technique in Production and Deployment has the greatest breadth of the *WAYS* it impacts the adversary**
- **→ Using this technique *ACROSS* the Acquisition Lifecycle reduces the adversary's presence the most**

Approved for Public Release;
Distribution Unlimited. Case Number 17-3169

# Visual Comparison of Mitigation Opportunities in MSA vs P&D

Materiel Solutions Analysis

Production & Deployment



| Acquisition Lifecycle | Resiliency Mitigations | Adversary Goals: Acquire Info | Develop tools | Deliver Attack | Initial Exploit | Controlling attack | Executing Attack | Maintain Presence | Defender Goals in O&S: Reduce attacks | Limit attack | Gain/Share Info |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Material Solutions Analysis | **Non-Persistence** | | | | | | | | | | |
| | Non-Persistent Information – Reduce availability of information about sy development | | | | | | | | | | |
| | Non-Persistent Services – Reduce the chance the adversary has corrupted environment to gain information | | | | | | | | | | |
| | Non-Persistent Connectivity – reduce the means to get the information ab developments | | | | | | | | | | |
| | **Privilege Restriction** | | | | | | | | | | |
| | Privilege Management – reduce the number of resources accessible with causing the adversary to invest more time and effort | | | | | | | | | | |
| | Privilege-Based Usage Restrictions – cause the adversary to expend more credentials | | | | | | | | | | |
| | Dynamic Privileges – increase the difficulty for the adversary in gaining | | | | | | | | | | |
| | **Realignment** | | | | | | | | | | |
| | Restriction – reduce the paths (via risky functionality or connectivity) use | | | | | | | | | | |
| | **Segmentation/Isolation** | | | | | | | | | | |
| | Predefined Segmentation – reduces adversary's ability to exfiltrate and the amount of data that can be exfiltrated – limiting the amount of information they can gain | x | | | | | | x | x | | |
| | Dynamic Segmentation/Isolation – contains the adversary's activities (such as the insertion of malware in running processes and control of compromised processes) limiting what they can do to gain information | x | | | | | | x | x | | |
| | **Unpredictability** | | | | | | | | | | |
| | Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials | x | | | | | | x | x | | |
| | **Deception** | | | | | | | | | | |
| | Dissimulation/disinformation – provide the adversary with false information so the attacks developed are ineffective in O&S | | | | | x | x | x | | x | x |
| | Misdirection – diverting attacks to a honeynet environment, enables defenders to analyze attack TTPs for future defense, eliminates attacks in this phase before they are passed to the next Acquisition lifecycle, and provides information about adversary targets | | | | x | x | x | x | x | x | x |
| | **Diversity** | | | | | | | | | | |
| | Architectural Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective | | x | | x | x | x | x | x | x | |
| | Design Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective | | x | | x | x | x | x | x | x | |
| | Command, Control and Communications Path Diversity – increase the defender's ability to remove attackers by using uncompromised communications channels once defenders become aware of exploit | | | | | | | x | x | x | |
| | Supply chain diversity – adversary must use more time and effort to compromise more supply chains or accept that there will only be a subset of target components compromised | | | x | x | | | | x | x | |
| | **Dynamic Positioning** | | | | | | | | | | |
| | Functional Relocation of Sensors – increase the likelihood of detecting adversary by tailoring sensor location this also makes it harder for the adversary to maintain their presence | | | | | x | x | x | | x | |
| | Distributed Functionality – increase the number of elements the adversary must compromise to deny or corrupt functionality | | | | | x | | x | | x | |
| | **Dynamic Representation** | | | | | | | | | | |
| | Dynamic Mapping and Profiling – identify software and components that do not conform to policy requirements or that are behaving in unexpected ways | | | | | x | | x | | x | x |
| | Dynamic Threat Modeling – reveal patterns and trends in adversary behaviors to share with O&S phase | | | | | x | | x | | x | x |
| | Mission Dependency and Status Visualization – identify consequences of adversary execution to share with O&S phase | | | | | | x | | | x | x |
| | **Non-persistence** | | | | | | | | | | |
| | Non-Persistent Information – limit the adversary's presence from delivery through maintenance by limiting the time information is available | | | x | x | x | x | x | x | x | |
| | Non-Persistent Services – limit the adversary's presence from delivery through maintenance by limiting the time the adversary can exploit a service | | | x | x | x | x | x | x | x | |
| | Non-Persistent Connectivity – limit the adversary's presence from delivery through maintenance by limiting the time paths into the environment are available | | | x | x | x | x | x | x | x | |

| Acquisition Lifecycle | Resiliency Mitigations | Attacker Goals: Acquire Info | Develop tools | Deliver Attack | Initial Exploit | Controlling attack | Executing Attack | Maintain Presence | Defender Goals in O&S: Reduce attacks | Limit attack | Gain/Share Info |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Production and Deployment | **Analytic Monitoring** | | | | | | | | | | |
| | Monitoring and Damage Assessment – Defenders obtain indications and warnings of adversary activities to share later in the Acquisition Lifecycle | | | x | | x | | x | | x | x |
| | Sensor Fusion and analysis – exposes adversary activity allowing defenders to gain information about the adversary attacks and share them with later Acquisition lifecycle phases | | | | | x | | x | | x | x |
| | Malware and Forensic Analysis – provide the defenders with the adversary's TTPs and capabilities | | | x | x | x | | x | | x | x |
| | **Coordinate Defense** | | | | | | | | | | |
| | Technical Defense-in-Depth – degrades the attackers' ability to initiate, control, execute or maintain attacks because they must develop attacks against multiple defensive technologies deployed concurrently | | | | x | x | x | x | x | x | |
| | Coordination and Consistency Analysis – reduce the attackers' ability to use unintended consequences or unforeseen dependences to disruptions to initiate exploits | | | | | x | x | x | x | x | |
| | **Deception** | | | | | | | | | | |
| | Dissimulation/disinformation – provide the adversary with false information so the attacks developed are ineffective in O&S | | | | | x | x | x | | x | x |
| | Misdirection – diverting attacks to a honeynet environment, enables defenders to analyze attack TTPs for future defense, eliminates attacks in this phase before they are passed to the next Acquisition lifecycle, and provides information about adversary targets | | | | x | x | x | x | x | x | x |
| | **Diversity** | | | | | | | | | | |
| | Architectural Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective | | x | | x | x | x | x | x | x | |
| | Design Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective | | x | | x | x | x | x | x | x | |
| | Command, Control and Communications Path Diversity – increase the defender's ability to remove attackers by using uncompromised communications channels once defenders become aware of exploit | | | | | | | x | x | x | |
| | Supply chain diversity – adversary must use more time and effort to compromise more supply chains or accept that there will only be a subset of target components compromised | | | x | x | | | | x | x | |
| | **Dynamic Positioning** | | | | | | | | | | |
| | Functional Relocation of Sensors – increase the likelihood of detecting adversary by tailoring sensor location this also makes it harder for the adversary to maintain their presence | | | | | x | x | x | | x | |
| | Distributed Functionality – increase the number of elements the adversary must compromise to deny or corrupt functionality | | | | | x | | x | | x | |
| | **Dynamic Representation** | | | | | | | | | | |
| | Dynamic Mapping and Profiling – identify software and components that do not conform to policy requirements or that are behaving in unexpected ways | | | | | x | | x | | x | x |
| | Dynamic Threat Modeling – reveal patterns and trends in adversary behaviors to share with O&S phase | | | | | x | | x | | x | x |
| | Mission Dependency and Status Visualization – identify consequences of adversary execution to share with O&S phase | | | | | | x | | | x | x |
| | **Non-persistence** | | | | | | | | | | |
| | Non-Persistent Information – limit the adversary's presence from delivery through maintenance by limiting the time information is available | | | x | x | x | x | x | x | x | |
| | Non-Persistent Services – limit the adversary's presence from delivery through maintenance by limiting the time the adversary can exploit a service | | | x | x | x | x | x | x | x | |
| | Non-Persistent Connectivity – limit the adversary's presence from delivery through maintenance by limiting the time paths into the environment are available | | | x | x | x | x | x | x | x | |
| | **Privilege Restriction** | | | | | | | | | | |
| | Privilege Management – cause the adversary to expend more time and effort to get credentials to deliver, initiate, control and execute the attack as well as maintain their presence | | | x | x | x | x | x | x | x | |
| | Privilege-Based Usage Restrictions – cause the adversary to expend more time and effort to get credentials to do anything in the environment | | | x | x | x | x | x | x | x | |
| | Dynamic Privileges – increase the difficulty for the adversary in gaining credentials | | | x | x | x | x | x | x | x | |
| | **Redundancy** | | | | | | | | | | |
| | Protected Backup and Restore - reduce threat of backups being corrupted | | | | | | | x | x | | |
| | **Segmentation** | | | | | | | | | | |
| | Predefined Segmentation – reduces adversary's ability to initiate exploit, control the malware, execute attacks and maintain their presence | | | | x | x | x | x | x | | |
| | Dynamic Segmentation/Isolation – contains the adversary's activities (such as the insertion of malware in running processes and control of compromised processes) limiting the adversary's ability to initiate exploit, control the malware, execute attacks and maintain their presence | | | | x | x | x | x | x | | |
| | **Substantiated Integrity** | | | | | | | | | | |
| | Integrity Quality checks – detect the presence of compromised components and remove them from the environment reducing the number of exploits and possibility of information exfiltration | | | x | | | | | x | | |
| | Provenance Tracking – detect the adversary's attempts to deliver compromised components and remove them from the environment | | | x | | | | | x | | |
| | Behavior Validation – identify the presence of compromised component in the environment | | | | x | x | x | x | x | x | |
| | **Unpredictability** | | | | | | | | | | |
| | Temporal Unpredictability combined with non-persistence – increase the difficulty for the adversary in to deliver malware, initiate the exploit and gain enough control to impact O&S | | | x | x | x | x | x | x | x | |
| | Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials | | | x | x | x | x | x | x | x | |
| | Contextual unpredictability combined with integrity quality checks – make it more difficult for the adversary to emulate components and get compromised components into fielded system | | | | x | | | x | x | | |

# Production & Deployment vs Operations & Support

- **Analytic Monitoring – gather fuse & analyze threat intelligence data to identify vulnerabilities, find adverse indications and identify damage**
  - *Production & Deployment*: enables defenders to obtain information about attacks - information used to enhance current defenses, share tactical information with and develop new defenses for O&S
  - *Operations & Support:* enables defenders to detect the presence of the adversary (usually during adversarial attacks or activities the adversary uses to maintain their presence)

Adversary has already acted

- **Diversity – use heterogeneity to minimize attacks exploiting common vulnerabilities**
  - *Production & Deployment*: cause the adversary to use more time and effort to get into and stay in the environment – In this phase there are more opportunities to use and implement diversity
  - *Operations & Support: similar to P&D in effect however there are few opportunities to use this technique in this phase*

Limited Opportunities



MITRE

# Combined Cyber Resiliency Mitigations for P&D and O&S (1)

Key
- P&D
- O&S
- Both

| Resiliency Mitigations | Attacker Goals | | | | | | | Defender Goals O&S | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Acquire Info | Develop tools | Deliver Attack | Initial Exploit | Control attack | Executing Attack | Maintain | Reduce attacks | Limit attack | Gain/Share Info |
| **Adaptive Response** | | | | | | | | | | |
| Dynamic Reconfiguration – making configuration changes during operations makes it harder for the adversary to control malware limiting the success of attacks | | | | | y | y | y | | y | |
| Dynamic Resource Allocation – changes the resources available for the adversary to exploit | | | | | y | y | y | | y | |
| Adaptive Management – changing how defensive mechanisms are used based on changes in the operational environment or threat environment forces the adversary to continue adapting to changes in the environment | | | | | y | y | y | | y | |
| **Analytic Monitoring** | | | | | | | | | | |
| Monitoring and Damage Assessment – Defenders obtain indications & warnings of adversary activities to share with later Aq phases | | | x | | x | y | b | | x | b |
| Sensor Fusion and analysis – exposes adversary activity allowing defenders to gain information about the adversary attacks and share them with later Acquisition lifecycle phases | | | | | x | y | b | | x | b |
| Malware and Forensic Analysis – provide the defenders with the adversary's TTPs and capabilities | | | x | x | x | y | b | | x | b |
| **Coordinate Defense** | | | | | | | | | | |
| Technical Defense-in-Depth – degrades the attackers' ability to initiate, control, execute or maintain attacks because they must develop attacks against multiple defensive technologies deployed concurrently | | | | x | b | b | b | x | b | |
| Coordination and Consistency Analysis – reduce the attackers' ability to use unintended consequences or unforeseen dependences to disruptions to initiate exploits | | | | | b | b | b | x | b | |
| **Deception** | | | | | | | | | | |
| Dissimulation/disinformation – provide the adversary with false information so the attacks developed are ineffective in O&S | | | | | x | x | x | | x | x |
| Misdirection – diverting attacks to a honeynet environment, enables defenders to analyze attack TTPs for future defense, eliminates attacks in this phase before they are passed to the next Acquisition lifecycle, and provides information about adversary targets | | | | x | x | x | x | x | x | x |
| **Diversity** | | | | | | | | | | |
| Architectural Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective | | x | | x | x | b | x | x | b | |
| Design Diversity/Heterogeneity – adversary must use more time and effort to develop tools that work across diverse implementations and initial exploit may not be as effective | | x | | x | x | b | x | x | b | |
| Command, Control and Communications Path Diversity – increase the defender's ability to remove attackers by using uncompromised communications channels once defenders become aware of exploit | | | | | | | b | x | b | |
| Supply chain diversity – adversary must use more time and effort to compromise more supply chains or accept that there will only be a subset of target components compromised | | | x | x | | y | | x | b | |

# Combined Cyber Resiliency Mitigations for P&D and O&S (2)

Key
- P&D
- O&S
- Both

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Dynamic Positioning** | | | | | | | | | | | |
| Functional Relocation of Sensors – increase the likelihood of detecting adversary by tailoring sensor location this also makes it harder for the adversary to maintain their presence | | | | | b | b | b | | b | | |
| Distributed Functionality – increase the number of elements the adversary must compromise to deny or corrupt functionality | | | | | b | | b | | b | | |
| **Dynamic Representation** | | | | | | | | | | | |
| Dynamic Mapping and Profiling – identify software and components that do not conform to policy requirements or that are behaving in unexpected ways | | | | | x | | b | | b | b | |
| Dynamic Threat Modeling – reveal patterns and trends in adversary behaviors to share with O&S phase | | | | | x | | b | | x | b | |
| Mission Dependency and Status Visualization – identify consequences of adversary execution to share with O&S phase | | | | | | x | | | b | b | |
| **Non-persistence** | | | | | | | | | | | |
| Non-Persistent Information – limit adversary's presence ( delivery through maintenance) by limiting the time information is available | | | x | x | b | b | b | b | b | | |
| Non-Persistent Services – limit the adversary's presence from delivery through maintenance by limiting the time the adversary can exploit a service | | | x | x | b | b | b | b | b | | |
| Non-Persistent Connectivity – limit the adversary's presence from delivery through maintenance by limiting the time paths into the environment are available | | | x | x | b | b | b | b | b | | |
| **Privilege Restriction** | | | | | | | | | | | |
| Privilege Management – cause the adversary to expend more time and effort to get credentials to deliver, initiate, control and execute the attack as well as maintain their presence | | | x | x | b | b | b | b | b | | |
| Privilege-Based Usage Restrictions – cause adversary to expend more time & effort to get credentials to do anything in environment | | | x | x | b | b | b | b | b | | |
| Dynamic Privileges – increase the difficulty for the adversary in gaining credentials | | | x | x | b | b | b | b | b | | |
| **Redundancy** | | | | | | | | | | | |
| Protected Backup and Restore - reduce threat of backups being corrupted | | | | | | | b | x | y | | |
| **Segmentation** | | | | | | | | | | | |
| Predefined Segmentation – reduces adversary's ability to initiate exploit, control malware, execute attacks and maintain presence | | | | x | b | b | b | x | y | | |
| Dynamic Segmentation/Isolation – contain adversary's activities (such as the insertion of malware in running processes and control of compromised processes) limiting the adversary's ability to initiate exploit, control malware, execute attacks & maintain presence | | | | x | b | b | b | x | y | | |
| **Substantiated Integrity** | | | | | | | | | | | |
| Integrity Quality checks – detect the presence of compromised components and remove them from the environment reducing the number of exploits and possibility of information exfiltration | | | x | | | y | | b | | | |
| Provenance Tracking – detect adversary's attempts to deliver compromised components and remove them from the environment | | | b | | | y | | b | | | |
| Behavior Validation – Identify the presence of compromised component in the environment | | | | x | x | x | b | x | b | | |
| **Unpredictability** | | | | | | | | | | | |
| Temporal Unpredictability combined with non-persistence – increase the difficulty for the adversary in to deliver malware, initiate the exploit and gain enough control to impact O&S | | | x | x | b | b | b | x | b | | |
| Temporal Unpredictability – combine with Dynamic Privileges – increase the difficulty for the adversary in gaining credentials | | | x | x | b | b | b | x | b | | |
| Contextual unpredictability combined with integrity quality checks – make it more difficult for the adversary to emulate components and get compromised components into fielded system | | | | x | y | y | b | b | y | | |