HIGH VALUE TARGET

An adversarial viewpoint to identify

High Value Targets

for increased Cyber Resilience

Francesco Chiarini
Founder & Chief Researcher, High Value Target ™

HIGH VALUE TARGET

About me

- Mastermind of High Value Target ™ Methodology
- Founder of the ISSA Cyber Resilience SIG
- Co-author World Economic Forum “Cyber Resilience Index”
- Co-author ASIFMA “Data Vaulting Considerations”
- Creator of the „Cyber Resilience Officer” concept
- Advisor to the UK CMORG Data Vault Cloud Architecture
- Speaker @ MITRE, FS-ISAC, FIRST, ISACA, ISSA, LSEG et al
- Designed and led the PepsiCo Cyber Fusion Center
- ISSA Volunteer of the Year (2021)
- US Consumer Brands Association Innovation Award (2018)
- Holds SABSA, GCED, ISO22301, CEH, EnCase et al

HIGH VALUE TARGET

Zero Trust Tenets Highlight Specific Cyber Resiliency Design Principles

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network locations.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Source: NIST SP 800-207

Structural Cyber Resiliency Design Principles

Limit the need for trust. 1 2 3	Control visibility and use. 1 2 3 4 6	Contain and exclude behaviors. 1 2 3 4	Layer defenses and partition resources.
Plan and manage diversity.	Maintain redundancy.		Make resources location-versatile.
Leverage health and status data. 5 7	Maintain situational awareness. 5 7		Manage resources (risk-) adaptively. 4 6 7
Maximize transience.	Determine ongoing trust-worthiness. 4	Change or disrupt the attack surface.	Make unpredictability and deception user-transparent.

HIGH VALUE TARGET

Agenda

Problem Statement

What are High Value Targets

What Can You Do With It

Key Takeaways


Resilience is about
being able to stand
despite the odds.

Problem Statement

- Obsolete “Crown Jewels” approaches endorsed by traditional Business Impact Analysis (BIA)
- Inability to focus defenses where they matter most, hindering cyber risk reduction
- Lack of skills to provide the required oversight to design and assure High Value Assets’ trustworthiness

Desired Outcome

Environment that impedes the attacker and increases their cost.

Confidently recover or restore to a trusted state quickly.

HIGH VALUE TARGET

High Value Assets & Critical Software

"A High Value Asset (HVA) is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business."

Since 2015, the Federal Government's High Value Asset initiative has ensured focus on the protection of the Federal Government's most critical and high impact information and information systems.

Executive Order 14028 issued in 2021 to direct NIST to define "critical software": any software that has, or has direct software dependencies upon, one or more components with at least one of certain key attributes.

Understanding Advanced Threat Actors

HIGH VALUE TARGET

Sophisticated and motivated

- Targets “critical infrastructure”
- Targets control plane
- Targets defensive capabilities
- Targets Crown Jewels
- Targets “undervalued” assets

NIST 800-30 Threat Source Capability Model Profile

Intent	4-5
Capability	4-5
Opportunity	4-5

MITRE ATT&CK TTPs (sample)

- T1591: Gather Victim Org Info
- T1587: Develop Capabilities
- T1195: Supply Chain Comp.
- T1072: Sw. Deployment Tools
- T1562: Impair Defenses
- T1553: Subvert Trust Controls
- T1561: Disk Wipe
- T1485: Data Destruction
- T1490: Inhibit Sys. Restoration

HIGH VALUE TARGET

Categories of High Value Targets

"Critical Infrastructure" Assets

Mission critical and / or complex dependencies.

- Domain Name System
- Backup & Storage
- Email (inc. Exec Email)
- Virtual Desktop Infrastructure

Control Plane Components

Management consoles, privileged operations, sensitive controls & instructions.

- Client Mgmt Tools
- Configuration Automation Console
- Network Mgmt Tools
- Antivirus Mgmt Console

Protective, Investigative & Response Tools

Defensive and response capabilities to withstand.

- Network Access Control
- Endpoint Detection & Response
- Intrusion & Detection Prevention
- Security Orchestration & Automation

Most Valued Data (+Crown Jewels)

Significant informational value of stored or transit data.

- Corporate Directories
- Identity & Access Mgmt Tools
- Critical Business Apps
- Databases, Repositories

HIGH VALUE TARGET

Attributes of High Value Targets

Pre-compromise

Provides Stealth

Provides the ability to bypass detection tools

Internal Prospecting

Provides full visibility into the control plane

External Exposure

Located in accessible zones for initial compromise

Does it…?

Compromise

Stores Secrets

Stores secrets that can be stolen or abused

Infiltrate Comms

Allows access to defender communication channels

Impair Defense

Allows to impair protect, investigative and response abilities of defenders

Can you …?

Post-compromise

Tamper Prone

Could be weaponized to support malicious activities

Inhibit Restoration

Provides ability to impair backup & restore capabilities

Stores Data

Provides access to highly valuable or large amount of data

Widespread Presence

Exists on multiple layers & provides ability to establish global foothold

HIGH VALUE TARGET

High Value Target Methodology

*"While **Endpoint Config & Management** is considered low from a business impact criticality perspective, in terms of Cyber Resilience, its compromise could be weaponized due to the levels of privilege and widespread nature, required for it's designed use."*

*"**Directory services** must be observed as a key element to an adversary's operations from a Cyber Resilience perspective, as it may grant the adversary multiple avenues of cyber terrain manipulation, defense evasion & access to defense critical data or assets."*

Goal: identify the inherent impact of the capabilities these assets provide to an unpredictable adversary.

Target Name	Critical Infrastructure	Control Plane	Defensive Tools	Critical Data Solutions	Score
Directory Services	✓	✓	✓	✓	**4**
Endpoint Config & Management		✓	✓		**2**

HIGH VALUE TARGET

High Value Target Methodology

Internal Prospecting

Main avenue for **recon, enumeration, priv. escalation, and pivoting** due to its key, central domain management role within an enterprise environment.

Widespread Presence

Global pervasiveness & inherit trust mechanisms may be leveraged for **large scale malware distribution** or **malicious terraforming**

Tamper Prone

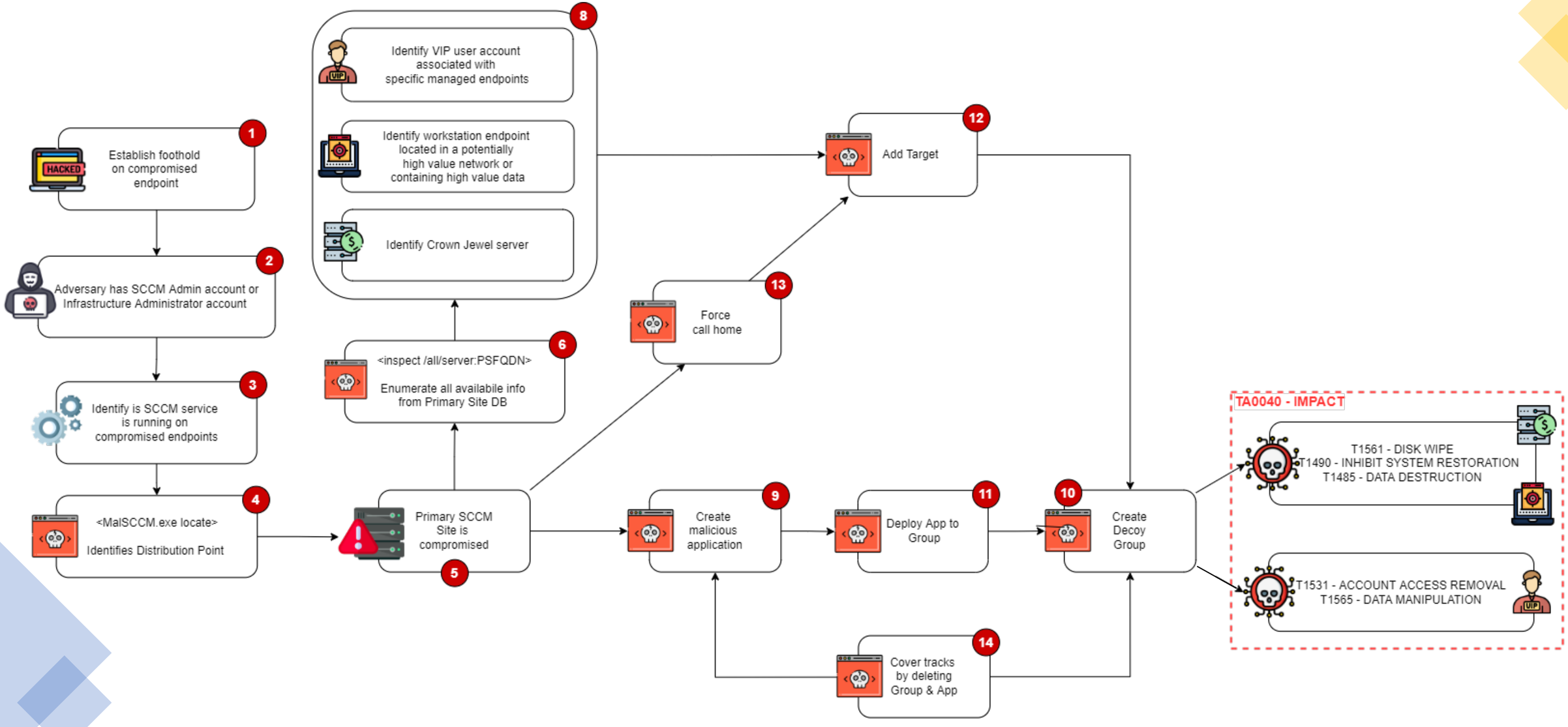
GPOs can be weaponized for a series of malicious activities, such as **establishing persistence , impairing defenses** and **malware distribution.**

Tamper Prone

Software Patching & Deployment capabilities can be weaponized for a series of malicious activities, such as **establishing persistence , lateral movement** and **malware distribution.**

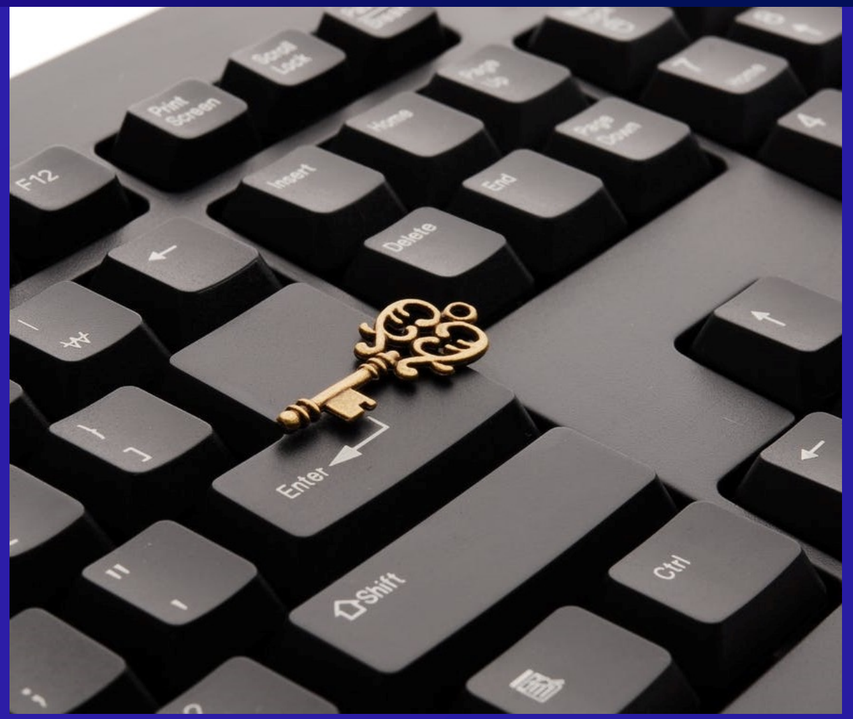
	Pre-compromise			Compromise			Post-compromise				
Target Name	Provides Stealth	Internal Prospecting	External Exposure	Stores Secrets	Infiltrate Comms.	Blindsides Defense	Tamper Prone	Inhibits Restoration	Stores Data	Widespread Presence	Score
Directory Services	8	8	5	8	5	2	8	5	5	8	6.2
Endpoint Config & Management	8	5	5	5	2	2	8	5	2	8	5

Threat Scenario for HVTs



Special thanks to Phil Keeble @ Nettitude for developing the MalSCCM tool

Key Takeaways



OBJECTIVE

Focus defenses where they matter most

= increase readiness vs unknown, unpredictable adversaries.

- Increase understanding of cyber terrain by applying HVTM
- Encourage defenders & operational resilience to think "Security Architecture"
- Bring Cyber Resilience to life:

Think High Value Targets

Establish a Cyber Resilience Officer

Write a Cyber Resilience Blueprint

What Next

- Encouraging industry adoption
- Expanding our R&D
- Influencing the standards
- Strenghtening partnerships

francesco@highvaluetarget.org

www.linkedin.com/in/chiarini

www.highvaluetarget.org

Research partner:

The Chertoff Group

Collaborating with:

- *MITRE*
- *NIST*
- *ENISA*
- *Sheltered Harbor*
- *OASIS Open*

High Value Target ™

- HVTM (assets) ✓
- HVTM (data, roles, vendors)
- HVT Structured Assessment
- HVT Analysis & Testing

R&D

- HVTM ServiceNow module
- OASIS STIX integration
- NIST CPE mappings
- MITRE CREF integration

Cyber Resilience Officer

- Educational course & dojos
- HVT organizational playbook
- Cyber Resilience Blueprint

Ready · Beta testing · In-flight · Planned

Appendix

High Value Target Methodology

Guiding Design Principles

1. The methodology focuses on inherent impact, hence on these attributes that are intrinsic to the object* itself and do not depend on mitigating controls in place;
2. The attributes of each object are subject to change, hand in hand with major technological progress or evolution of cyber adversaries' sophistication;
3. The methodology provides quantitative measures in terms of low / moderate / high value that an adversary aims to seek for and then leverage;
4. The methodology produces an outcome in form of a label which can be intended as a binary value about whether the object is or isn't a High Value Target;
5. The methodology is an evolvable product which could be leveraged in a multitude of contexts like risk assessments, threat modeling, security operations and more;
6. The High Value Target objects and attributes are for the community hence feedback is encouraged and considered in order to strengthen the methodology and ensure fit-for-use;
7. The High Value Target methodology is an extension of authoritative publications ranging from NIST, MITRE, WEF and more. It is not meant to be a proprietary framework of its own.

* Object = asset, role, third party, data

High Value Target Sample Use Cases

HIGH VALUE TARGET

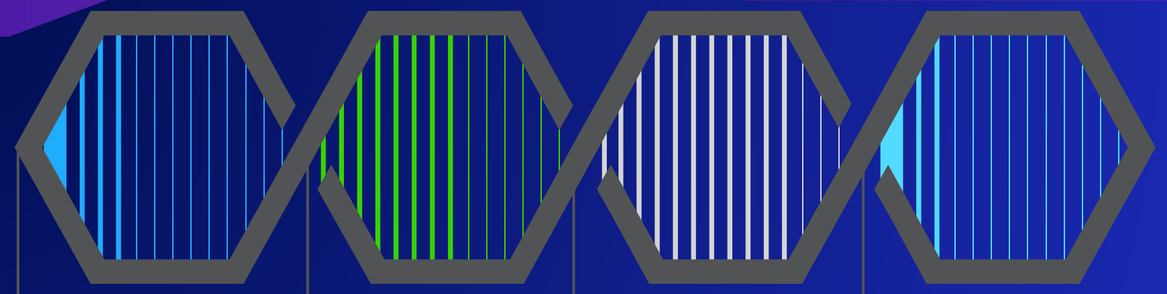
Cyber Threat Intelligence
- Threat actors focus vs HVTs
- Ingest HVT data from CPE / CVE

Cyber Fusion & adversary proximity
- Enhanced monitoring for HVTs
- 3rd Party and Insider Threat for HVTs

Operational Resilience
- Consideration of HVTs in important business services
- Blast-radius view from crown jewels

Cyber risk quantification
- Inclusion of HVTs in „risk to group”
- Enhanced HVTs control baselines

Offensive security
- Enrich of target selection process
- Enhance reports’ risk summary



Anticipate
Fortify & Surveill

Withstand
Impede Intruders

Recover
Immune & Self-Repairing

Evolve
Adapt & Transform

Cyber Courses of Action
- Include HVTs in IR and DR plans
- Awareness of HVT architecture

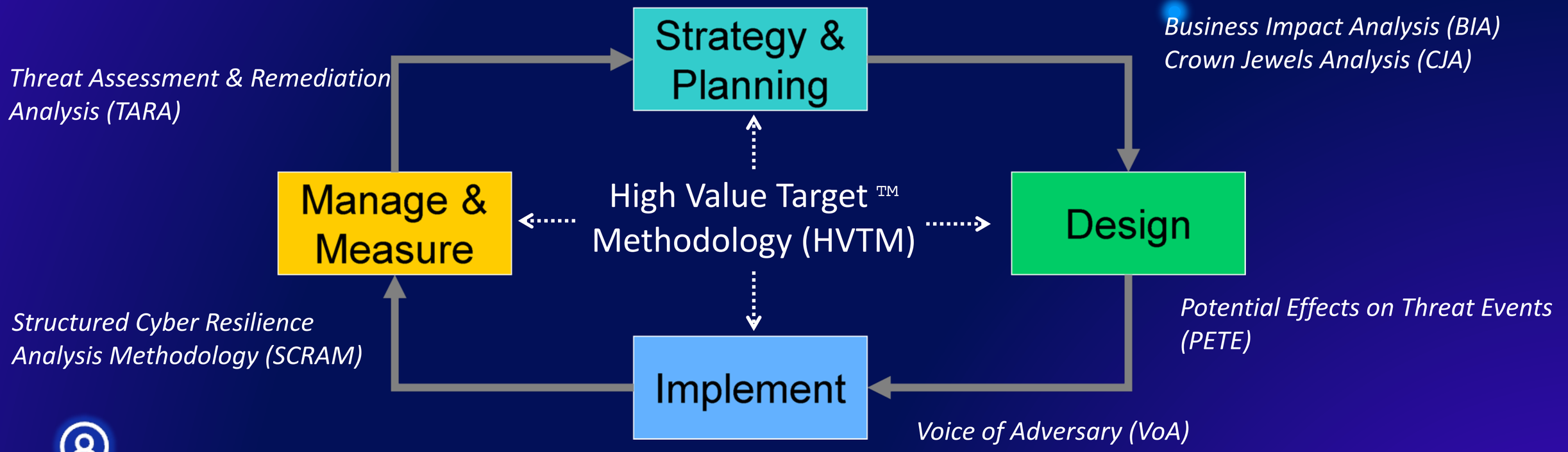
TTX and scenario testing
- Remove assumptions on HVTs
- Adopt extreme but plausible TTX

Towards an increased Cyber Resilience posture

We cannot protect today’s organizations with yesterday’s frameworks and tools yet wanting to show a low-risk appetite for cyber threats. We need an evolved framework to identify cyber risk accounting for advanced adversarial actions.

HIGH VALUE TARGET

Organizational Process for High Value Targets

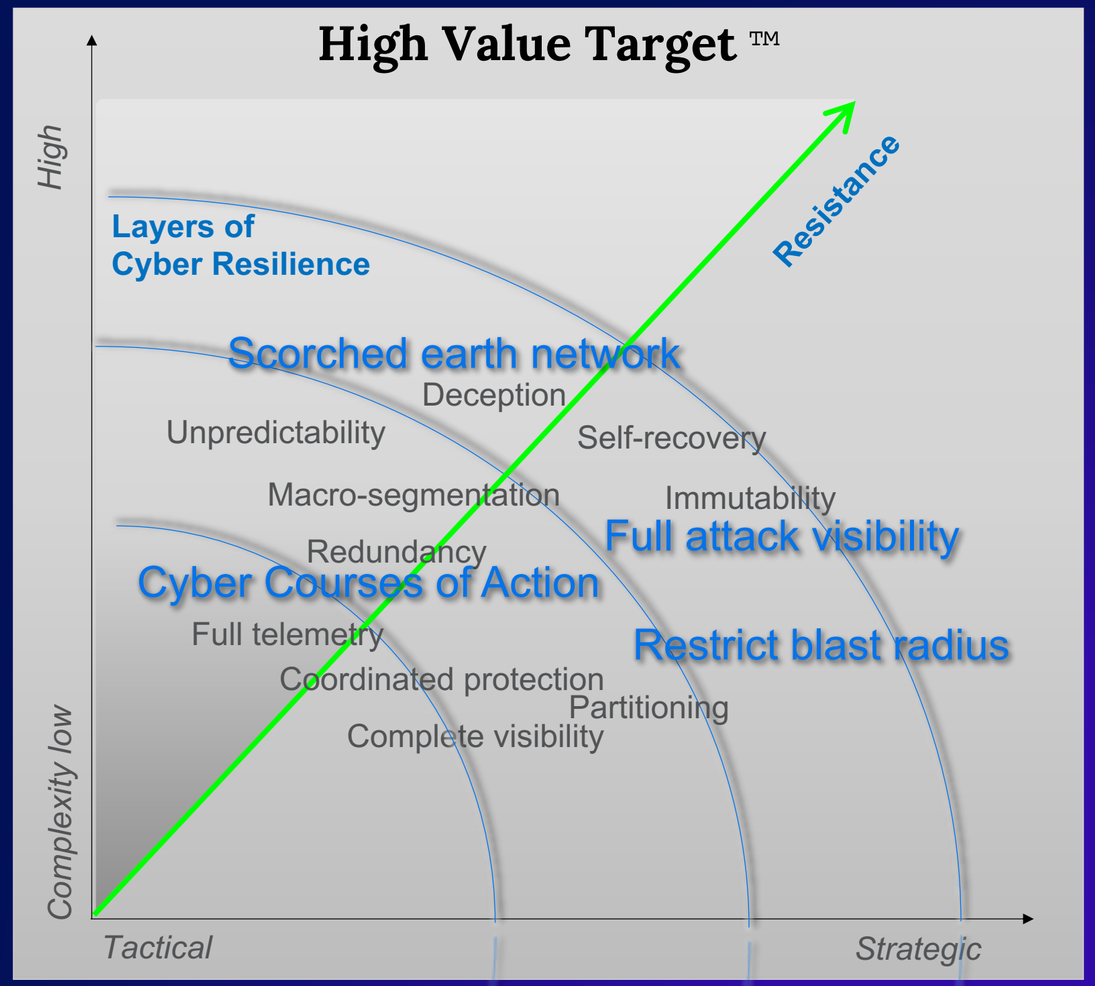


- **Threat-Informed Defenders & Engineers**
- **Enterprise Security Architects**
- **Operational Resilience Specialists**
- **Offensive Security Personnel**
- **Third Party Security Assessors**
- **Risk & Compliance Specialists**

HIGH VALUE TARGET

What is Cyber Resilience

Cybersecurity is based on NIST 800-53. Cyber Resilience is based on NIST 800-160.	*Requirements*
Cybersecurity protects high value assets (business). Cyber Resilience protects even high value targets (adversary).	*Assets*
Cybersecurity focuses on severe but plausible scenarios. Cyber Resilience on extreme but plausible.	*Threats*
Cybersecurity focuses on reducing likelihood of occurrence. Cyber Resilience focuses on reducing magnitude of impact.	*Risk*

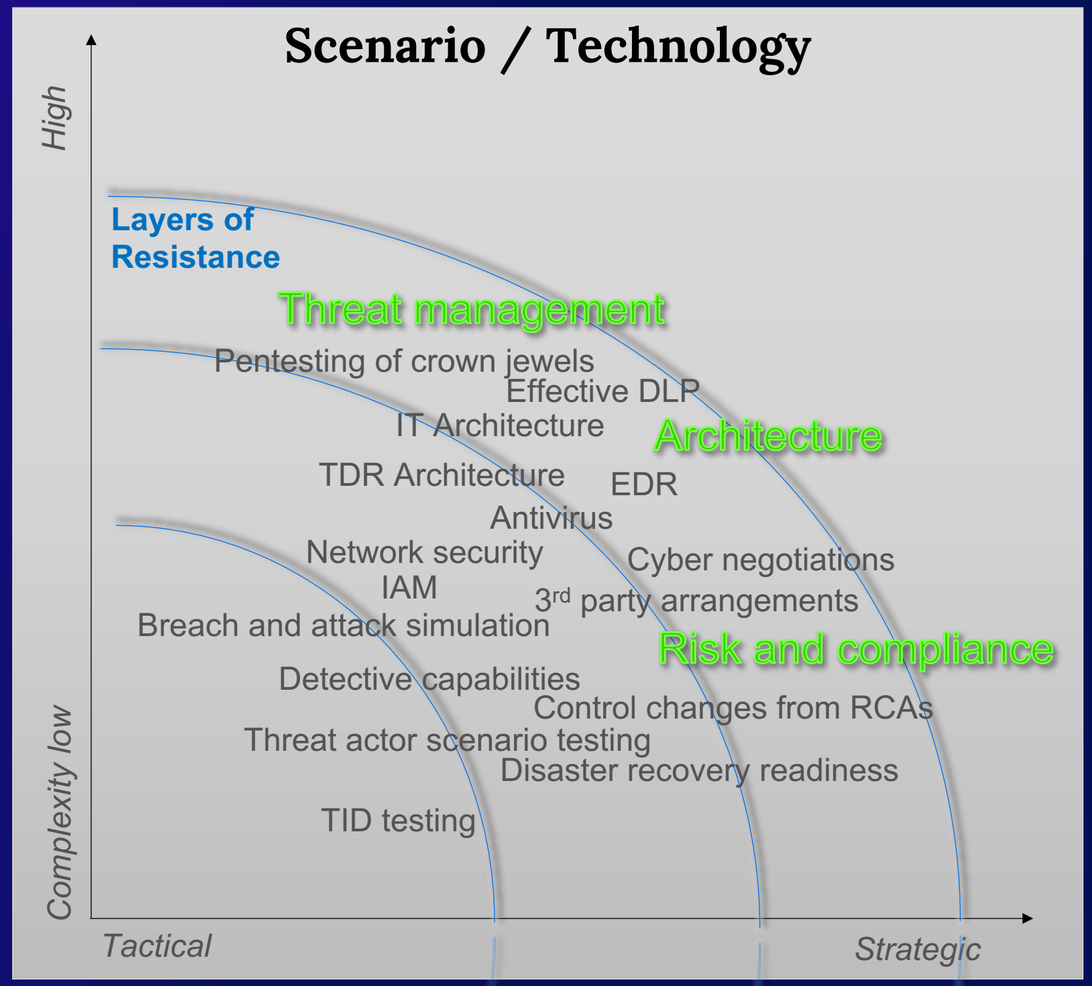


HIGH VALUE TARGET

Traditional Cyber Security

Prioritized themes: Key controls, Crown Jewels, Threat scenarios

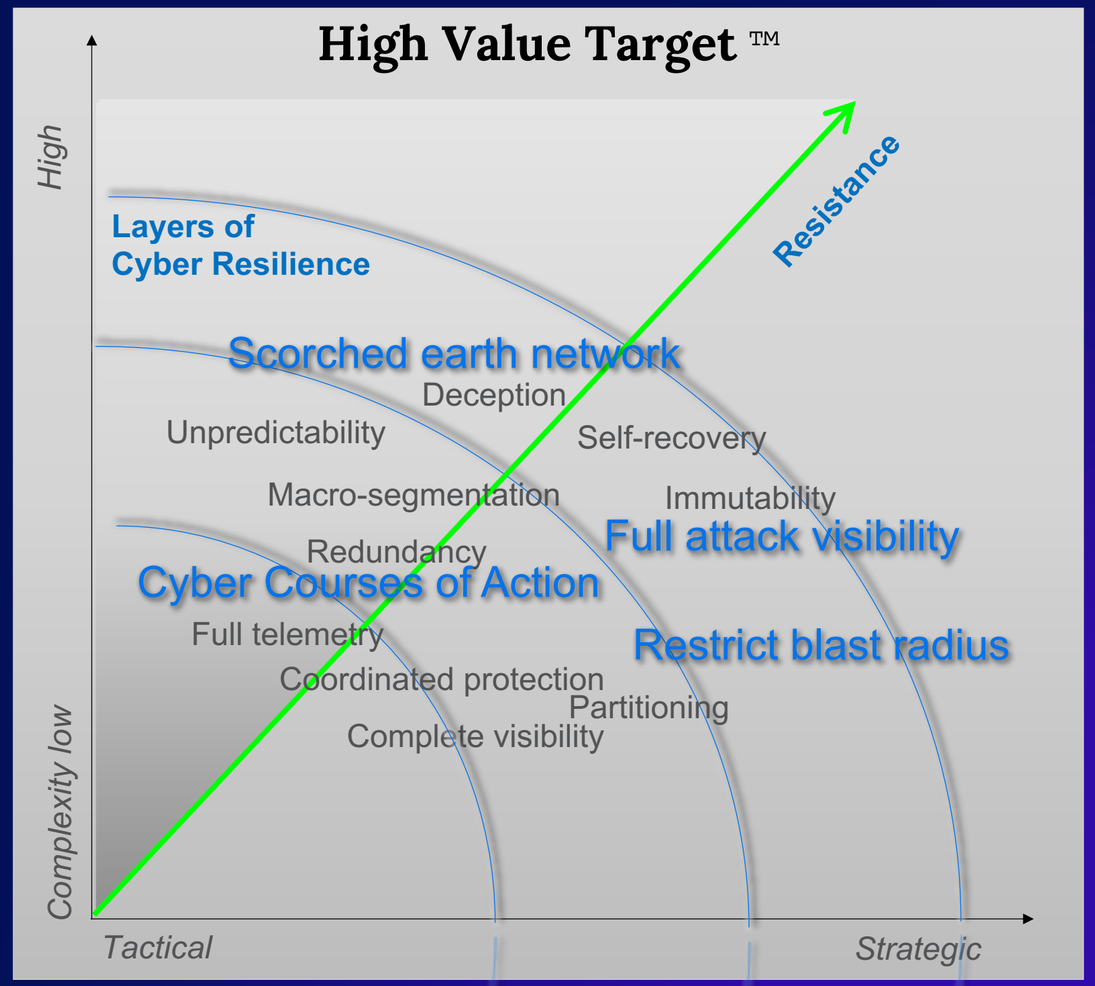
Traditional: Identify, Protect, Detect, Respond, Recover



Cyber Resilience

Environment that impedes the attacker and increases their cost

Reliably recover to a trusted state quickly.



HIGH VALUE TARGET

References

1. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, National Institute of Standards and Technology, 2021 - https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final
2. Cyber Resiliency Engineering Framework, MITRE, 2012 - https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework
3. MITRE ATT&CK Framework, MITRE, 2013 - https://attack.mitre.org/
4. Cyber Lexicon, Financial Stability Board, 2018 - https://www.fsb.org/wp-content/uploads/P121118-1.pdf
5. Secure High Value Assets, Cybersecurity and Infrastructure Security Agency, 2020 - https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf
6. Glossary, National Institute of Standards and Technology, 2019 - https://csrc.nist.gov/glossary/term/advanced_persistent_threat
7. The CARVER Target Analysis and Vulnerability Assessment Methodology, 2018 - https://en.wikipedia.org/wiki/CARVER_matrix
8. Operational resilience: Impact tolerances for important business services, Bank of England, 2021 - https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=D6335BA4712B414730C697DC8BEB353F3EE5A628
9. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin, 2011 - https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
10. Structured Cyber Resiliency Analysis Methodology, MITRE, 2016 - https://www.mitre.org/news-insights/publication/structured-cyber-resiliency-analysis-methodology
11. Guide for Conducting Risk Assessments NIST SP 800-30 v1, NIST, 2012 - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
12. SABSA Enterprise Security Architecture Lifecycle, 1995 - https://sabsa.org/sabsa-executive-summary/
13. TARA and Crown Jewels Analysis, MITRE, 2011 - https://www.mitre.org/sites/default/files/2021-10/pr-11-4982-tara-methodology-and-description.pdf
14. Voice of Adversary (VoA), NIST Special Publication 800-160, Volume 2, NIST, 2019 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
15. Potential Effects on Threat Events (PETE) Analysis, MITRE, 2022 - https://ieeexplore.ieee.org/document/9850337/