CYBER RESILIENCE MANIFESTO

www.cyberresiliencemanifesto.eu

Powered by:

rd

<resilient>defense

ABOUT

This manifesto encapsulates the core of cyber resilience and aims to ease the professional life of cyber resilience practitioners who -like us- face challenges explaining what cyber resilience is about.

Our goal in crafting the Cyber Resilience Manifesto is to disseminate knowledge on cyber resilience that informs, educates, and motivates practitioners to integrate cyber resilience, thereby enhancing organizational survivability against cyber threats.

We drafted this manifesto to aid in modernizing and potentially standardizing (or at least establishing consistency for) cyber resilience practices. After evaluating various frameworks, we decided that focusing on strategic capabilities offers the most direct route to tangible organizational benefits.

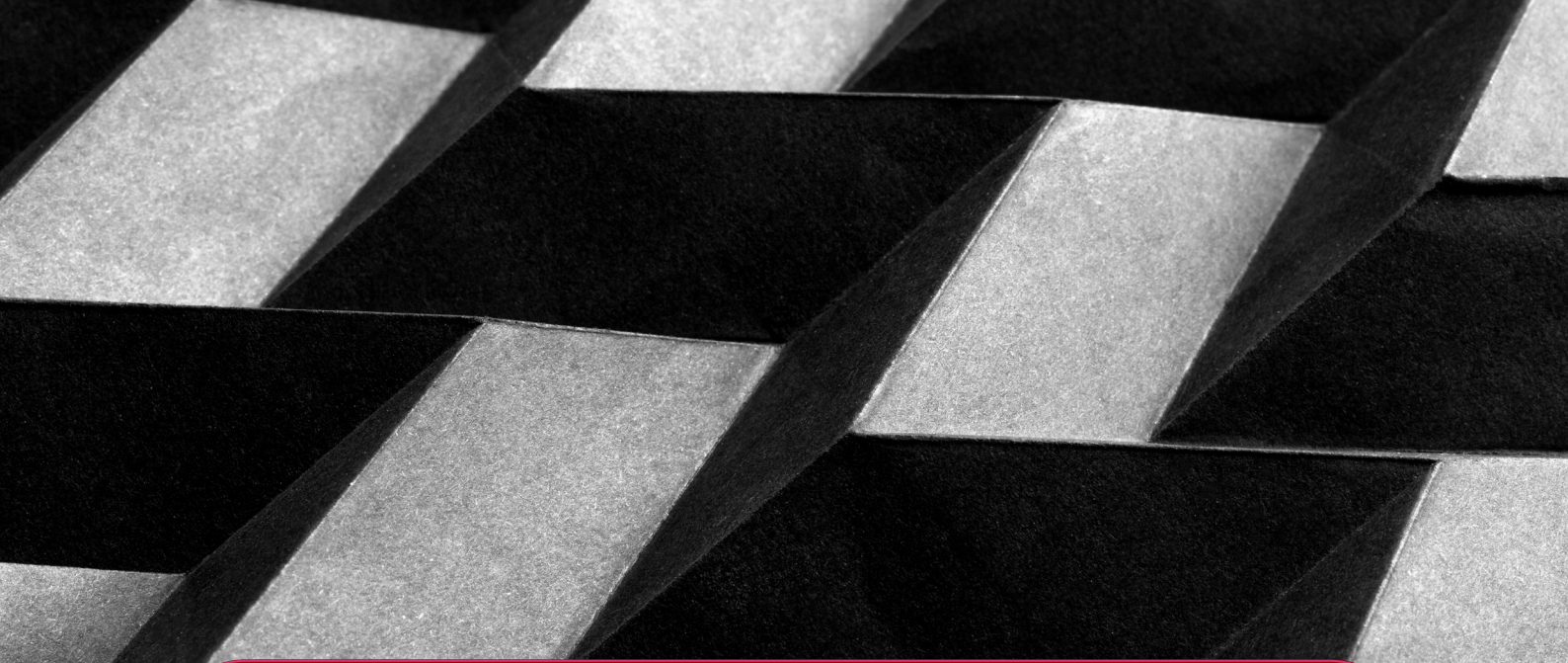
Although our group collectively possesses extensive experience in cyber resilience, we do not claim to have all the answers. We invite reviews and insights from others in the cyber resilience field. Feedback can be shared via email at team@resilientdefense.com, and we will assess the contributions to refine and expand the manifesto.

Thanks to <resilient>defense for producing the Cyber Resilience Manifesto.

Visit the online version and share it within your network:
www.cyberresiliencemanifesto.eu

This document encapsulates the core of cyber resilience and solves the challenge of explaining what cyber resilience is really about.

SUMMARY



CYBER RESILIENCE MANIFESTO

Cyber resilience is an extension of information security and an evolution of operational resilience. It is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Developing Cyber-Resilient Systems is a NIST Special Publication which is considered the most authoritative resource available today.

An organization's cyber resilience efforts primarily aim to implement strategies and tactics that ensure the survivability of mission-critical functions before, during, or after a coordinated, destructive cyber-attack. Such cyber resilience strategies and tactics require capabilities to address the continuously evolving risks from advanced and unpredictable adversaries. This implies expanding threat scenario definition and modeling beyond "severe but plausible" and focusing on capable and motivated adversaries introducing "extreme but plausible" threat scenarios. The defender's goal should be to make it costly and difficult for these advanced adversaries to break into the organization's environment and execute such an attack.

A fundamental step to achieving cyber resilience is identifying and understanding the organization's critical assets, i.e., critical information assets (data) and information systems (applications), processes, roles, and third parties that are high value assets, and developing plans to become resilient-by-design. For such identification to be effective, it must focus on the assets' inherent impact and consider both the business objectives (Voice of the Customer) and the adversary's (Voice of the Adversary).

Business resilience is the outcome of well-executed information security, operational resilience, and cyber resilience and is defined by the World Economic Forum as "the ability of an organization to transcend any stresses, failures, hazards, and threats to its cyber resources within the organization and its ecosystem, such that the organization can confidently pursue its mission, enable its culture, and maintain its desired way of operating."

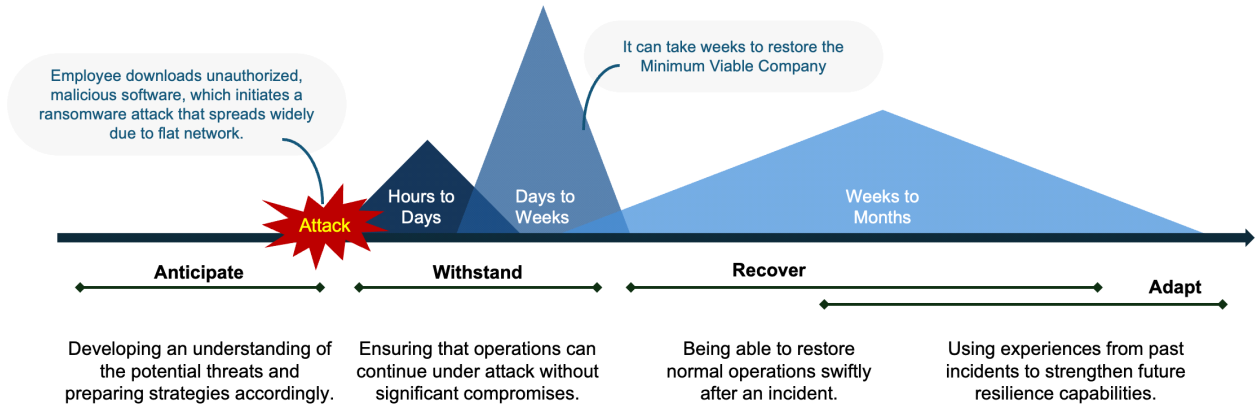
The Cyber Resilience Manifesto is authored by Francesco Chiarini, Patrick Lechner, and Calin Gheorghiu and is produced by <resilient>defense—special thanks to Wim Stoffelen for the support.

References

Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST SP 800-160
National Institute of Standards and Technology
The Cyber Resilience Index: Advancing Organizational Cyber Resilience

DEFINITION

Cyber resilience is defined as an organization's ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. It requires resilient-by-design strategies across all four goals to achieve its ultimate and most fundamental goal: business resilience.



- To anticipate: developing an understanding of the potential threats and preparing strategies accordingly.
- To withstand: ensuring operations can continue under attack without significant compromises.
- To recover: restoring normal operations swiftly after an incident.
- To adapt: using experiences from past incidents to strengthen future resilience capabilities.

INFORMATION SECURITY VS CYBER RESILIENCE

Cyber resilience is a (1) extension of information security and a (2) evolution of operational resilience.

» Cyber resilience as an extension of information security:

Dimension	Information Security	Cyber Resilience
Assets	Information security focuses on protecting all assets, with a focus on high value assets (business view) and their availability loss	Cyber resilience focuses on protecting primarily high value targets (adversary view) and is concerned with CIA loss.
Threats	Information security focuses on "severe but plausible" threat scenarios involving adversaries who target the less protected and the most vulnerable.	Cyber resilience focuses on "extreme but plausible" threat scenarios against adversaries who may cause unknown harm to the whole organization.
Risks	Information security focuses on reducing the likelihood of occurrence and the likelihood of impact, limiting the adversary's ability to execute against their objectives.	Cyber resilience focuses on reducing the magnitude of impact, which specific security architecture and engineering practices can achieve. Resiliency recognizes that harm may occur and how to maximize mission achievement despite that.
Controls	Information security encompasses a comprehensive set of controls from NIST 800-53, around 1100 controls.	Cyber resilience extends the depth at which a smaller set of these controls from NIST 800-160 and 800-172, which count around 200 controls.

If your administrator can do it, an adversary can do it.

OPERATIONAL RESILIENCE VS CYBER RESILIENCE

» Cyber resilience as an evolution of operational resilience:

Dimension	Operational resilience	Cyber Resilience
Purpose	Operational resilience ensures the continuous functioning of all business operations during any type of disruption, focusing on the organization's ability to deliver essential services	Cyber resilience focuses on maintaining and rapidly restoring digital operations during and after cyber-attacks, explicitly targeting the security and availability of essential IT systems and services.
Preparedness	Operational resilience involves broad strategies that coordinate across departments to manage risks from any source, ensuring resilience in physical, personnel, and process aspects.	Cyber resilience employs information security measures outlined in NIST SP 800-160 and SP 800-172 to defend IT assets against specific cyber threats, focusing on a narrower, more technical scope of preparedness.
Recovery	Operational resilience targets overall business continuity, focusing on recovering full-service delivery, not just IT services. This includes ensuring that alternative business processes are ready and viable as outlined in NIST SP 800-34 or ISO22300.	Cyber resilience concentrates on technical recovery solutions, primarily from technology disruptions. It uses advanced response and recovery controls and goes beyond the traditional assumption that secondary arrangements (like backup systems or failovers) will operate effectively when primary systems fail.
Impact	Information security encompasses a comprehensive set of controls from NIST 800-53, around 1100 controls.	Cyber resilience extends the depth at which a smaller set of these controls from NIST 800-160 and 800-172, which count around 200 controls.

CRITICAL ASSETS

In a world of finite resources, irreducible uncertainty, and competing priorities, organizations must develop robust & accurate critical asset identification practices and determine the necessary layers of cyber resilience required for these systems. Critical assets are business or technical applications that underpin several key business processes. Compromise of these assets with impact on confidentiality, integrity, or availability may result in severe effects on the organization, including financial, reputational, operational, health and safety, strategic, and legal or regulatory consequences. Focusing defenses where they matter most must be a top priority for business and technology leaders alike, enabling organizations to maintain tactical superiority during a sophisticated cyber incident unfolding. Critical assets must be identified, designed, developed, implemented, and maintained appropriately, leveraging tailored cyber resilience best practices. This approach is particularly relevant when addressing the most advanced adversaries with the required levels of capability of executing highly targeted & orchestrated campaigns with potential long-term operational impact on organizations. These priority threat actors target not only the most vulnerable or least protected assets to carry out their mission. They develop tactical opportunities by attacking assets that maximize the chances of achieving campaign objectives, referred to as high value targets. Identifying, securing, and continuously governing high value targets substantially enhances an organization's cyber resilience. This approach allows you to allocate your security budget more effectively, ensuring that you neither overspend on controls for certain critical assets (crown jewels) nor underspend on others (high value targets).

As Alexander the Great said, "If you try to defend everything, you defend nothing."

CYBER RESILIENCE STRATEGY

A cyber resilience strategy recognizes that despite organizations' best protection measures, adversaries may succeed in breaching boundary defenses and further compromise a defender's system. When this situation occurs, organizations must employ countermeasures to detect, outmaneuver, confuse, deceive, mislead, and impede the adversary—that is, "removing the adversary's tactical advantage and protecting the organization's high value assets." To maintain confidence in the trustworthiness of an environment of operation, organizations should implement a continuous cyber resilience assurance cycle, which "is intended to identify where, how, and when cyber resiliency techniques can be applied to improve architectural resiliency against advanced cyber threats" (MITRE). The ten abilities that exhibit mastery of well-executed cyber-resilient strategies are:

» The organization can predict adversary attacks.

» The organization can prevent adversary attacks.

» The organization can prepare for adversary attacks.

» The organization can fight through cyberattacks.

» The organization can contain or defeat the adversary.

» The organization can determine damages caused by a cyber adversary.

» The organization can restore.

» The organization can determine reliability.

» The organization can transform existing processes and behavior.

» The organization can re-architect.

While operational resilience and information security prepare you against severe but plausible threat scenarios, cyber resilience prepares you for the tail-risk, black swan extreme but plausible.

CYBER RESILIENCE ARCHITECTURE

Five strategic pillars of cyber resilience find relevance in the way systems are architected. These concepts are well articulated NIST 800-160.

Limited organizational resources must be allocated where they can provide the greatest benefit. This results in a strategy of focusing first on critical assets and ensuring our environment is designed to favor defensive operations, limit attackers, and avoid saturation of response capabilities.

The threat landscape changes as adversaries evolve, but so do an organization's technology footprint and relevant processes. Agility and adaptability are essential components of the risk management strategy, which should be designed to accommodate the assumption that unexpected changes in the threat, technical, and operational environments will occur throughout the system's lifespan.

Defending a large attack surface is challenging and necessitates continuous efforts to monitor, analyze, and respond to anomalies. Reducing the attack surface lowers the costs associated with protection, and adversaries are forced to focus their efforts on a smaller set of locations, resources, or environments, which can be monitored and defended more effectively. Additionally, disrupting the attack surface is crucial to impede adversaries from gaining a foothold.

Systems and system components, ranging from chips to software/running services, can be compromised for extended periods without detection. Some compromises may never be detected. Across all levels of abstraction, systems must be designed to meet minimum performance and quality requirements across all operational states.

Sophisticated cyber adversaries dedicate time, effort, and resources to crafting and enhancing their tactics, techniques, and procedures (TTPs). They adapt based on emerging technologies, new applications of existing technologies, and insights gained from understanding the TTPs of defenders. Moreover, the tools developed by these advanced adversaries quickly become accessible to less skilled attackers. Consequently, systems and missions must maintain resilience against unforeseen attacks.

To become truly cyber resilient, you must architect the organization to prepare for the "unknown."

CYBER RESILIENCE OUTCOMES

A state-of-the-art cyber-resilient enterprise can achieve the following high-level outcomes:

1. Identify (and develop contingencies for) impacts and risks that emerge from its attack surface and the external threat landscape, then dynamically redefine defensive architecture mitigations to protect its critical assets.

2. Design its processes (risk, architecture, and more) to be resilient by default by identifying the goals, objectives, techniques, and approaches required

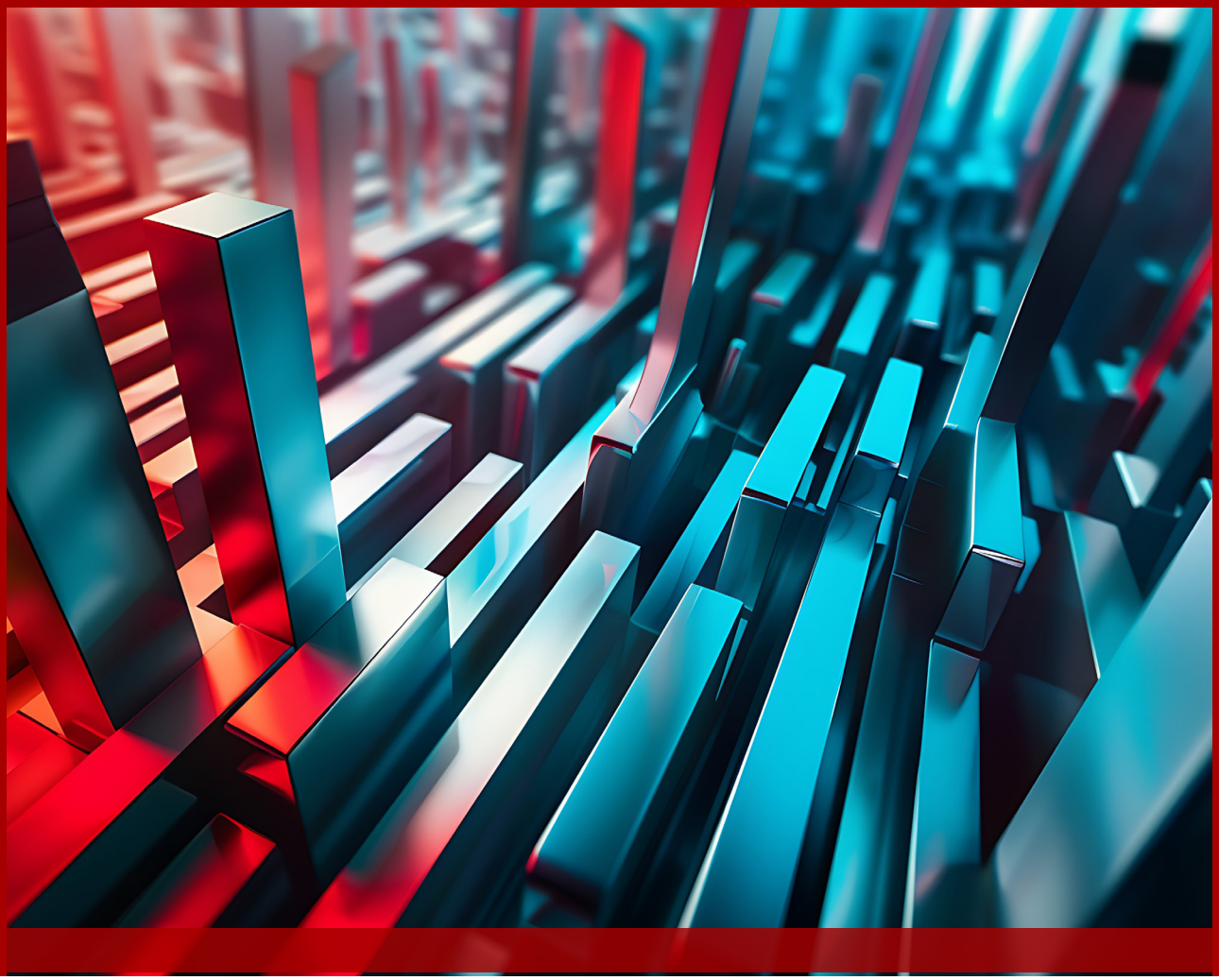
3. Identify and protect assets at risk of being weaponized against the company itself due to the architectural nature of these systems and maintain break-glass capabilities to recover in case of broad compromise.

4. Cultivate a resilience-conscious workforce and ensure personnel are prepared and equipped to respond to cyber threats, with the necessary resources tested, exercised, and readily accessible, fostering a workforce capable of effectively responding to and mitigating cyber incidents.

5. Identify (and address) lessons learned from other organizations that were believed to be resilient but were rendered operationally incapacitated by advanced adversaries.

6. Effectively measure capabilities and identify risks before they become material by tracking capabilities and developing business intelligence through information sharing & peer benchmarking.

Complexity is the enemy of good resilience.

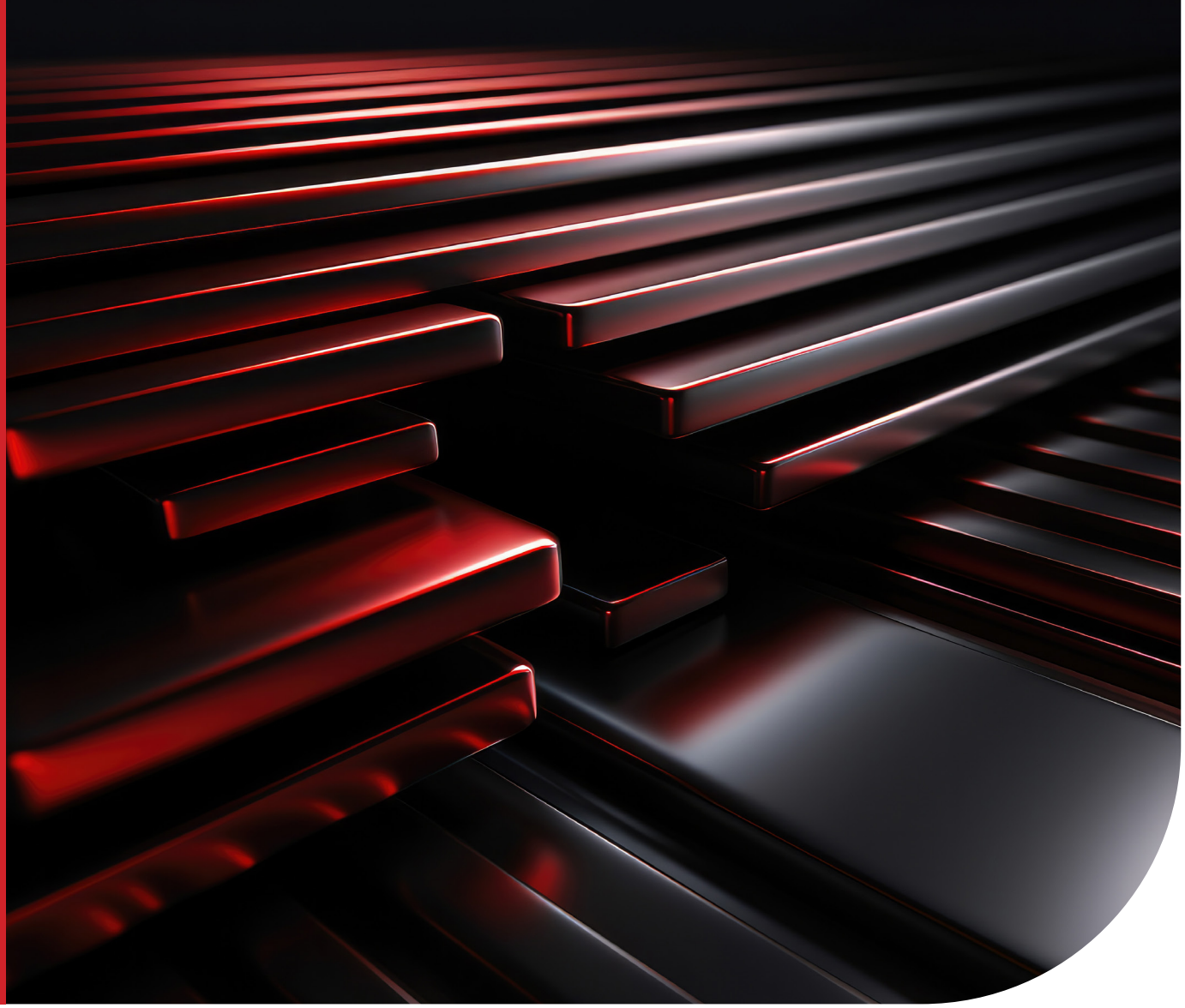


ACCOUNTABILITY FOR CYBER RESILIENCE

A robust cyber resilience strategy requires skillsets across operational resilience, information security, and cyber resilience. Therefore, successful cyber resilience programs are built by accountable cyber resilience practitioners who acknowledge the inevitability of breaches and focus on removing the adversary's tactical advantage. This process involves constant analysis, planning, and execution of cyber resilience techniques to improve architectural resiliency against advanced cyber threats. Cyber resilience as a competency: a set of abilities related to architecting, designing, developing, implementing, maintaining, and sustaining the trustworthiness of systems that use or are enabled by cyber resources to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, and attacks. While accountability for cyber resilience may span various roles depending on an organization's structure, a cyber resilience officer who is accountable for the organization's ability to manage cyber resilience and implement cyber resilience goals is a sound way forward. As such, a first step for any cyber resilience officer should be to advocate for ensuring the organization's most critical assets are properly identified, protected, continuously assessed, and governed.

Business resilience is an outcome of well-executed information security, operational resilience, and cyber resilience.

team@resilientdefense.com



CONTACT

Thanks to <resilient>defense for producing the Cyber Resilience Manifesto

Email:
team@resilientdefense.com

Website:
www.resilientdefense.com