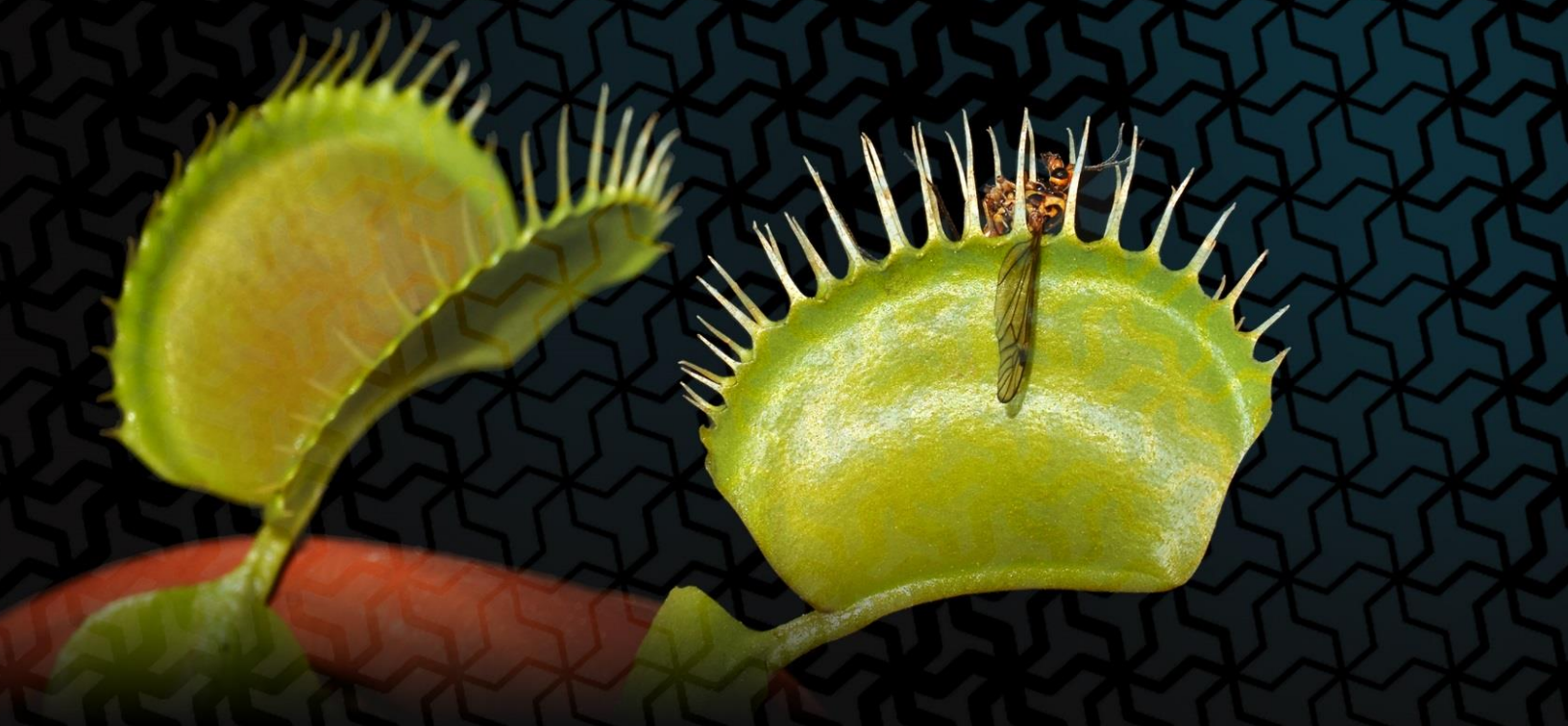
ACALVIO

# Acalvio Deception and the NIST Cybersecurity Framework 1.1

**January 2020**



## Background

The NIST Cybersecurity Framework 1.1 (CSF) is being widely adopted by organizations of all types as they seek to minimize risk. The CSF provides a technology-neutral reference to define, implement, and report on cybersecurity posture. Acalvio solutions are well-suited to support the Cybersecurity Framework, in particular the requirements related to detection of threats and modeling of adversaries.

### Highlights

- The NIST Cyber Security Framework (CSF) provides a reference for building and executing an InfoSec security policy and control set.
- Although originally created for critical national infrastructure, the CSF is now applied broadly across numerous industry segments.
- Acalvio ShadowPlex supports 14 NIST CSF controls, especially those related to detection and threat characterization.
- Acalvio meets the NIST CSF detection and response requirements in a more cost-effective and operationally efficient manner than alternative approaches.

## NIST Cybersecurity Framework Background

The NIST Cybersecurity Framework provides an approach to prioritize cybersecurity resources, make risk decisions, and take action to reduce risk. It was originally designed to be applied by operators of critical national infrastructure. However with technology becoming ubiquitous across industry sectors, organizations of all types are now leveraging the Framework to better organize, prioritize, and justify their IT security efforts.

The CSF avoids specifying technologies to be deployed to minimize risk, and instead focuses on processes and outcomes. That is, it speaks to how an organization should approach cyber risk management, and enumerates activities that are likely to produce desired states corresponding to acceptable risk levels.

The Framework is composed of three parts:

**Core**: The key element of the Framework, the Core is a list of cybersecurity activities and controls that are relevant across all industries.

**Implementation Tiers**: A set of four levels of rigor controls may be applied, ranging from “Partial” to “Adaptive”. Organizations should select the tier appropriate to the risks associated with the relevant assets, processes, or data being protected.

**Profiles**: In the context of the CSF, a profile is a description of the state of cybersecurity controls across a subset of the organization’s environment. It combines business requirements, risk tolerance, and resources with the Core controls. The CSF encourages the creation of both Current and Desired Profiles, so that a gap analysis can be performed to drive the roadmap for achieving the desired risk posture. Unlike the core controls and tiers, profiles are not explicitly defined in the CSF, but are created by the organization as it executes the framework. An organization may have multiple profiles, to reflect the variety of internal assets and the risk profile and resources associated with each.While compliance with the CSF is voluntary, adopting the framework establishes a solid and

defensible basis for claiming a reasonable level of attention and diligence with respect to information security.

## Overview of CSF Core Controls

The NIST Cybersecurity Framework 1.1 Core controls are organized into five "Functions" or high level outcomes: Identify, Protect, Detect, Respond, and Recover. Within these five functions are a total of 23 activity "Categories", under which numerous activities and controls ("Subcategories") are listed. The intent is that organizations will evaluate each of the controls within the Core against their assets and risk tolerance to arrive at their desired cybersecurity posture.

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management and Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

**The NIST Cybersecurity Framework - Core Functions and Categories**

## Acalvio Support for NIST Cybersecurity Framework

Acalvio's ShadowPlex Distributed Deception Platform is extremely well suited to supports the goals of the NIST Cybersecurity Framework. Acalvio delivers

- Fast and accurate incident detection
- Adversary engagement and forensics
- Threat response to retard attack propagation

Like the CSF, Acalvio starts with the premise that attacks will not just be initiated from outside the perimeter, but will be successful in penetrating the network. The key elements of the CSF are focused on detecting such events, which is exactly what Acalvio does. In fact it is difficult to imagine an effective CSF implementation without Acalvio, because there will otherwise inevitably be blind spots due to lack of complete coverage of possible attack methods and vectors.

A crucial aspect of threat detection in the NIST Framework is speed. It is well understood that most attacks go undetected for weeks or months, allowing the adversary to do significant damage before there is any response or mitigation. It is also well documented that most attacks do leave some form of forensic trail behind – the problem is that these clues are not obvious, and are drowned out in a sea of uncorrelated events and data. Acalvio solves this problem: events detected by ShadowPlex are very likely related to actual attacks, because the platform assets serve no legitimate purpose. This enables the rapid response essential to execute effective response and mitigation. Implementing Acalvio protects key assets by containing and controller the attacker early in the kill chain.

Acalvio deception-based detection is superior to alternative approaches such as behavioral analytics because it is both more accurate (few false positives) and more efficient and easier to deploy. Furthermore, what separates Acalvio from all other detection solutions is operational efficiency at scale. Acalvio's technology supports broad application across the internal estate, while minimizing both capital and ongoing expenses and effort. Legacy "Deception 1.0" honeypot solutions simply cannot be scaled or operated easily. Organizations do not have unlimited budgets for implementing cyber security, and the more efficiently they can deploy funds, the more effectively they can build a robust defensive architecture.

Acalvio is also relevant in the Response and Recovery portions of the CSF. ShadowPlex includes services that can contain an attacker within a constrained environment where he cannot access production assets. It can also deploy fake but attractive assets (e.g. file shares) that obfuscate valuable data and retard an attacker's progress.

The table below summarizes Acalvio's support for the NIST Cybersecurity Framework 1.1 controls. Acalvio supports 14 of the NIST CSF subcategories or controls, including four of the five high-level Functions. As Acalvio is primarily a detection solution, the major of support is in the Detect function, however controls are also supported in the Identify, Respond, and Recovery functional areas.

| NIST CSF 1.1 Subcategory (Control) | Acalvio ShadowPlex Support |
|---|---|
| **Identify (ID)** | |
| ID.RA-3: Threats, both internal and external, are identified and documented. | Using Deception 2.0 breadcrumbs and lures, Acalvio detects attacker activity in systems, servers and endpoints. Acalvio is also able to detect such activity through attempted communication to Acalvio decoys. Full documentation of attack actions and methods is automatically gathered. Based on those inputs detailed forensic information is obtained through deep engagement of the attacker's identity, techniques and motives. |
| ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | Acalvio delivers network-wide data related to device inventory and real-time threat activity, allowing organizations to assess both likelihood and potential impact. |
| | |
| **Detect (DE)** | |
| DE.AE-2: Detected events are analyzed to understand attack targets and methods | Acalvio collects and correlates event data from honeypot services (variable interaction decoys); root cause analysis (through attacker engagement and full stack decoys); incident forensics and packet analysis (deep engagement). Fluid Deception delivers highly credible decoys; breadcrumbs are monitored using advanced techniques including file entropy. |
| DE.AE-3: Event data are collected and correlated from multiple sources and sensors | Acalvio Deception Farms scale to support thousands of data sources throughout the environment. Solution integrations allow this data to be blended with other sources (e.g. SIEM) to provide a unified picture of the attack. |

| NIST CSF 1.1 Subcategory (Control) | Acalvio ShadowPlex Support |
|---|---|
| DE.AE-5: Incident alert thresholds are established. | Benchmark of normal activity across the environment is provided to determine proper alert thresholds. |
| DE.CM-1: The network is monitored to detect potential cybersecurity events. | Acalvio decoys monitor network activity to detect all unusual events that suggest compromise. ShadowPlex Reflections Engines allow specialized systems (e.g. medical or SCADA devices) to be replicated virtually to enhance realism in non-standard, high-value networks. Deception Farms technology supports broad deployments with minimal operational overhead and cost. |
| DE.CM-4: Malicious code is detected | Acalvio detects malicious code via detection of anomalous activity targeted at decoys or lures. |
| DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed | Connections, devices, and software activity on systems are all monitored by Acalvio. |
| DE.DP-3: Detection processes are tested | Red team or Penetration exercises can leverage Acalvio capabilities and integrations to test organizational detection efficacy. |
| | |
| **Respond (RS)** | |
| RS.AN-2: The impact of the incident is understood | Acalvio Adversary Behavior Analytics (ABA) examines an identified attack to better understand impact, including attack origination, machines compromised, and current attacker posture within the environment. Acalvio provides a complete audit trail of the attack, making it trivial to determine the earliest date of compromise. |
| RS.AN-3: Forensics are performed | Acalvio provides detailed information of subnets and hosts affected by an attack to inform the scope of forensics. It also provides detailed forensic information |

| NIST CSF 1.1 Subcategory (Control) | Acalvio ShadowPlex Support |
|---|---|
| | through deep engagement of the attacker's identity, techniques and motives. Depending on the type of attack and level of engagement, Acalvio can determine the external addresses or domains related to the incident. |
| RS.MI-1: Incidents are contained | The Acalvio Shadow Network, or False Apparent Network, can contain an attacker and prevent compromise of sensitive assets. |
| RS.MI-2: Incidents are mitigated | Acalvio can dynamically deploy lures relevant to an attacker's methods to obfuscate sensitive assets and delay attack propagation. |
| | |
| **Recovery (RC)** | |
| RC.RP-1: Recovery plan is executed during or after a cybersecurity incident | The Acalvio Shadow Network can be used to allow deep continuous attacker engagement during the incident, without compromising the security of production assets. Acalvio also can deploy counter measures to slow an attack and limit damage. |

*"The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience."*

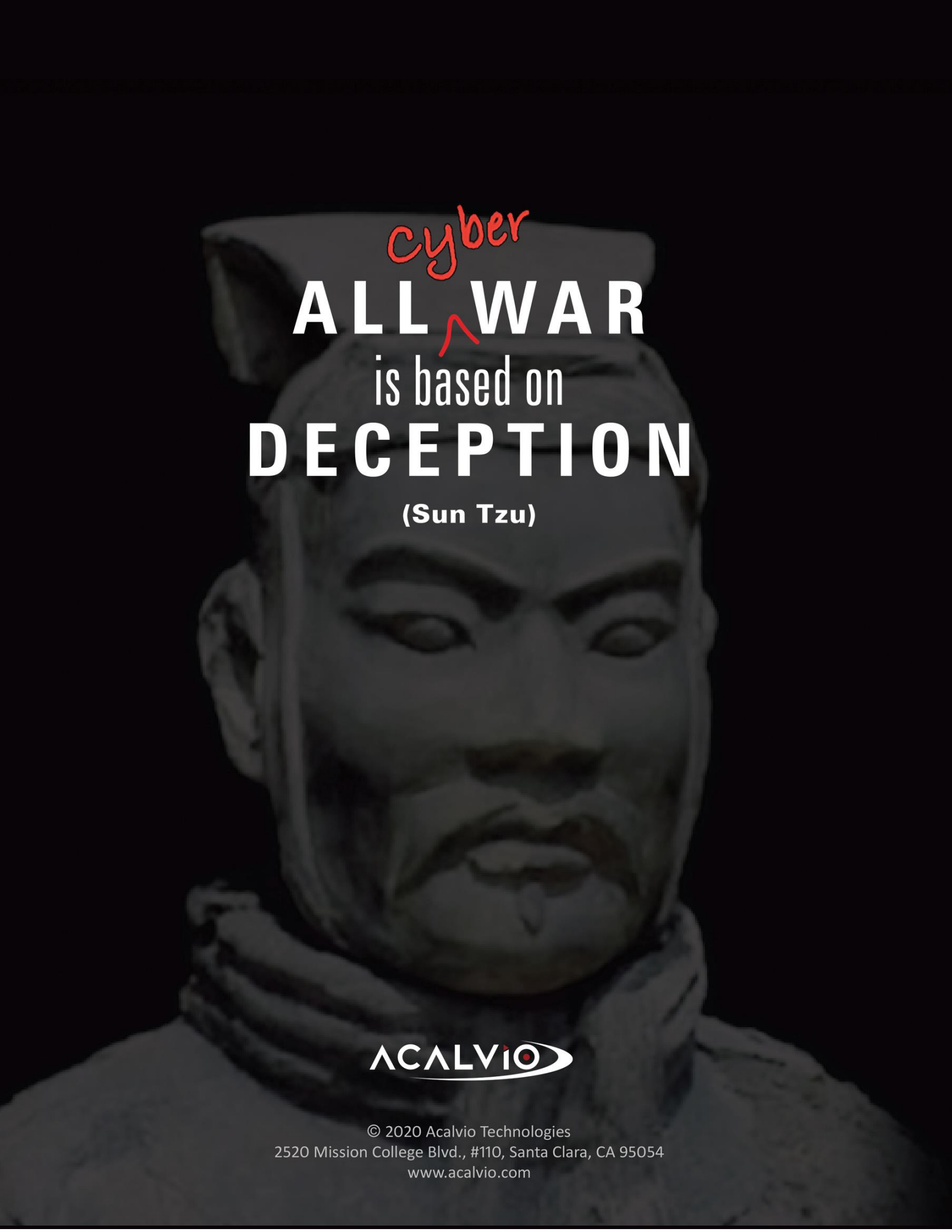
*NIST Cybersecurity Framework 1.1, 2018*

*"[The Framework] is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT)."*

*NIST Cybersecurity Framework 1.1, 2018*

*"Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment."*

*NIST Cybersecurity Framework 1.1, 2018*





2520 Mission College Blvd., #110, Santa Clara, CA 95054
www.acalvio.com