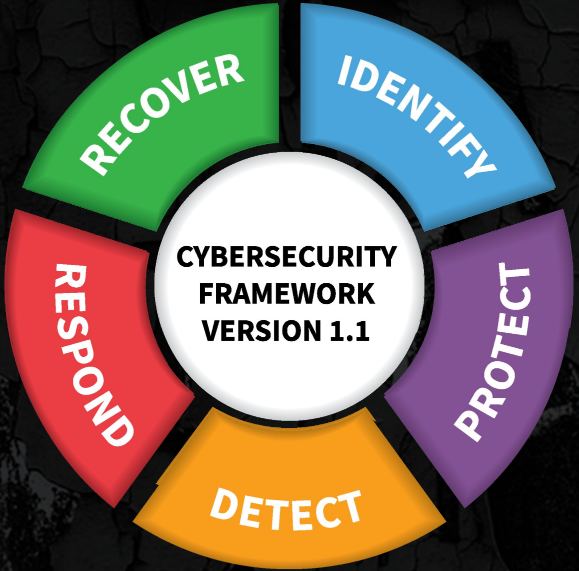


# DeNISTifying Cybersecurity

Leveraging A Proven Framework to Evolve Your Stack

HUNTRESS

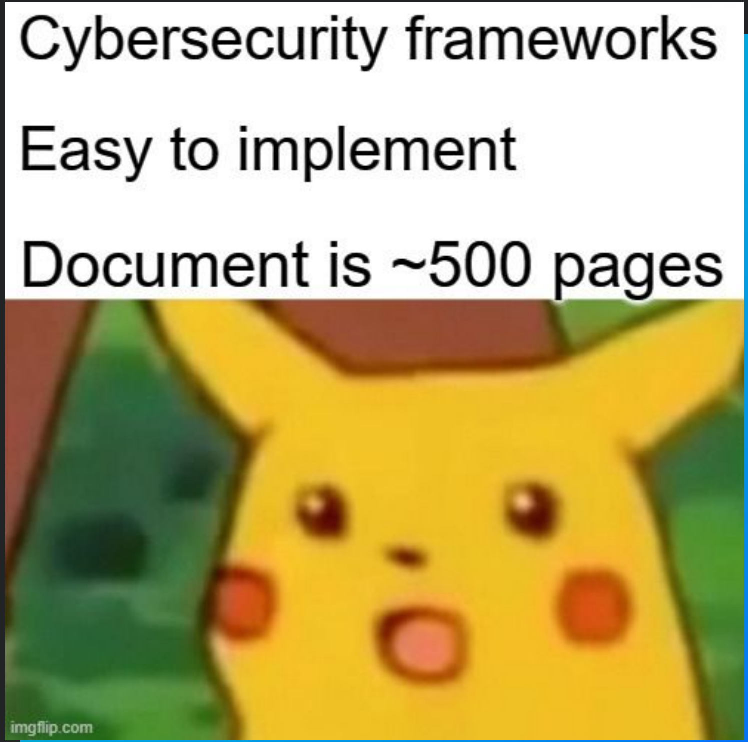
# Today’s Agenda

1. Introduction
2. NIST Cybersecurity Framework
3. CIS Controls v8
4. Takeaways

# 01

# Introduction

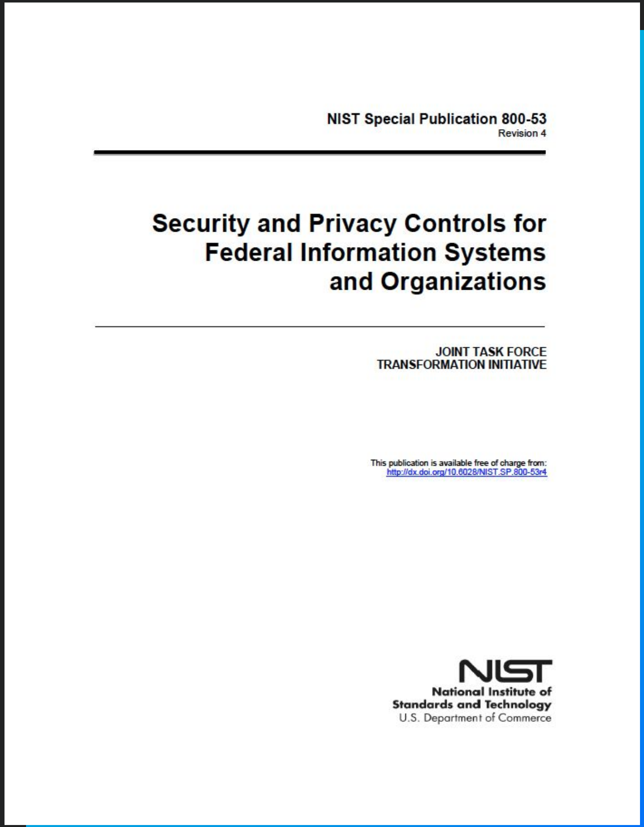
# NEED SOMETHING HERE–BUT WHAT?!!



# Light Reading

463 Page Document

Abstract:
This publication provides a catalog of security and privacy controls to protect organizational operations, organizational assets, individuals, and the Nation from a diverse set of threats. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk.



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for
Federal Information Systems
and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

# All the Controls

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AC-1 | AC-21 | AU-16 | CP-4 | IA-11 | MP-4 | PE-8 | PL-8 | RA-3 | SC-8 | SC-28 | SI-4 | SA-7 |
| AC-2 | AC-22 | AT-1 | CP-5 | IR-1 | MP-5 | PE-9 | PL-9 | RA-4 | SC-9 | SC-29 | SI-5 | SA-8 |
| AC-3 | AC-23 | AT-2 | CP-6 | IR-2 | MP-6 | PE-10 | PM-1 | RA-5 | SC-10 | SC-30 | SI-6 | SA-9 |
| AC-4 | AC-24 | AT-3 | CP-7 | IR-3 | MP-7 | PE-11 | PM-2 | RA-6 | SC-11 | SC-31 | SI-7 | SA-10 |
| AC-5 | AC-25 | AT-4 | CP-8 | IR-4 | MP-8 | PE-12 | PM-3 | CA-1 | SC-12 | SC-32 | SI-8 | SA-11 |
| AC-6 | AU-1 | AT-5 | CP-9 | IR-5 | PS-1 | PE-13 | PM-4 | CA-2 | SC-13 | SC-33 | SI-9 | SA-12 |
| AC-7 | AU-2 | CM-1 | CP-10 | IR-6 | PS-2 | PE-14 | PM-5 | CA-3 | SC-14 | SC-34 | SI-10 | SA-13 |
| AC-8 | AU-3 | CM-2 | CP-11 | IR-7 | PS-3 | PE-15 | PM-6 | CA-4 | SC-15 | SC-35 | SI-11 | SA-14 |
| AC-9 | AU-4 | CM-3 | CP-12 | IR-8 | PS-4 | PE-16 | PM-7 | CA-5 | SC-16 | SC-36 | SI-12 | SA-15 |
| AC-10 | AU-5 | CM-4 | CP-13 | IR-9 | PS-5 | PE-17 | PM-8 | CA-6 | SC-17 | SC-37 | SI-13 | SA-16 |
| AC-11 | AU-6 | CM-5 | IA-1 | IR-10 | PS-6 | PE-18 | PM-9 | CA-7 | SC-18 | SC-38 | SI-14 | SA-17 |
| AC-12 | AU-7 | CM-6 | IA-2 | MA-1 | PS-7 | PE-19 | PM-10 | CA-8 | SC-19 | SC-39 | SI-15 | SA-18 |
| AC-13 | AU-8 | CM-7 | IA-3 | MA-2 | PS-8 | PE-20 | PM-11 | CA-9 | SC-20 | SC-40 | SI-16 | SA-19 |
| AC-14 | AU-9 | CM-8 | IA-4 | MA-3 | PE-1 | PL-1 | PM-12 | SC-1 | SC-21 | SC-41 | SI-17 | SA-20 |
| AC-15 | AU-10 | CM-9 | IA-5 | MA-4 | PE-2 | PL-2 | PM-13 | SC-2 | SC-22 | SC-42 | SA-1 | SA-21 |
| AC-16 | AU-11 | CM-10 | IA-6 | MA-5 | PE-3 | PL-3 | PM-14 | SC-3 | SC-23 | SC-43 | SA-2 | SA-22 |
| AC-17 | AU-12 | CM-11 | IA-7 | MA-6 | PE-4 | PL-4 | PM-15 | SC-4 | SC-24 | SC-44 | SA-3 | |
| AC-18 | AU-13 | CP-1 | IA-8 | MP-1 | PE-5 | PL-5 | PM-16 | SC-5 | SC-25 | SI-1 | SA-4 | |
| AC-19 | AU-14 | CP-2 | IA-9 | MP-2 | PE-6 | PL-6 | RA-1 | SC-6 | SC-26 | SI-2 | SA-5 | |
| AC-20 | AU-15 | CP-3 | IA-10 | MP-3 | PE-7 | PL-7 | RA-2 | SC-7 | SC-27 | SI-3 | SA-6 | |

**NIST 800-53 has 256 security controls**

# The Great NIST Caveat

## Situations Requiring Potential Baseline Supplementation

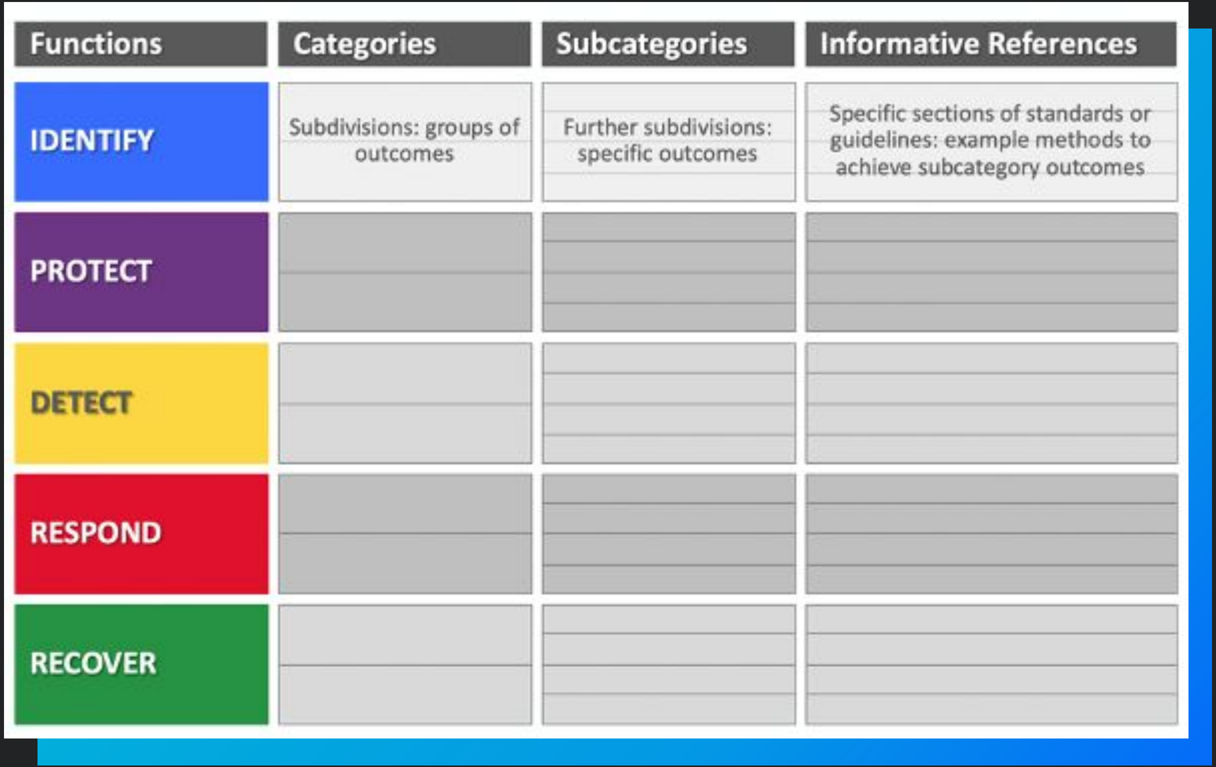
ADVANCED PERSISTENT THREAT

**Security control baselines do not assume that the current threat environment is one where adversaries have achieved a significant foothold and persistent presence.**

02

# NIST Cybersecurity Framework

# Framework Core



| Functions | Categories | Subcategories | Informative References |
|---|---|---|---|
| IDENTIFY | Subdivisions: groups of outcomes | Further subdivisions: specific outcomes | Specific sections of standards or guidelines: example methods to achieve subcategory outcomes |
| PROTECT | | | |
| DETECT | | | |
| RESPOND | | | |
| RECOVER | | | |

# IDENTIFY

- **Asset Inventory**
- **Governance, Risk, Compliance**
- **Vulnerability Scanning**

- Identification of assets: How can you defend what you don't know you (or your partners) have in their environments?
- Assets != Devices
    - Users
    - Data
    - Applications
    - Vendors
- Critical to achieve success throughout the CSF. (Strong Foundation)

# IDENTIFY Categories

- Asset Management: 6 subcategories
- Business Environment: 5 subcategories
- Governance: 4 subcategories
- Risk Assessment: 6 subcategories
- Risk Management Strategy: 3 subcategories
- Supply Chain Risk Management: 5 subcategories

# PROTECT

- AV/NGAV
- Firewalls
- DNS Filtering
- NAC / MFA
- Least Privilege
- Email Security
- Phishing Training
- Encryption
- IDS/IPS
- SIEM

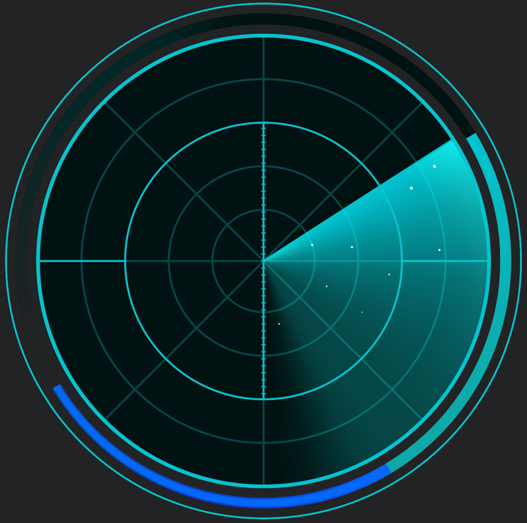
- Mostly technical controls.
- What amount of coverage is sufficient to limit or contain the impact of a cybersecurity incident?
- Don’t forget about physical security!

# PROTECT Categories

- Identity Management, Authentication and Access Control: 7 subcategories
- Awareness and Training: 5 subcategories
- Data Security: 8 subcategories
- Information Protection Processes and Procedures: 12 subcategories
- Maintenance: 2 subcategories
- Protective Technology: 5 subcategories

# DETECT

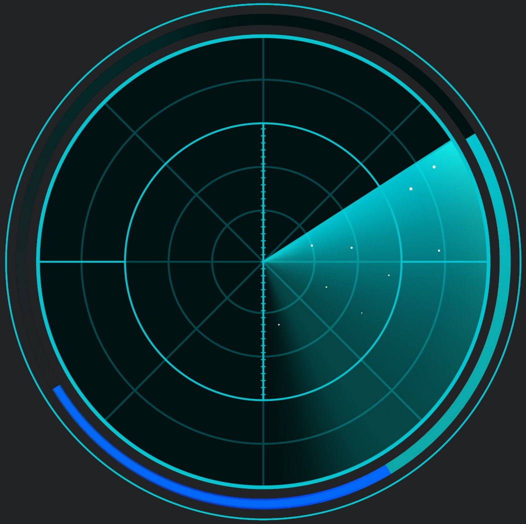
- Threat Hunting
- Endpoint Threat Detection
- Network Behavior Analysis
- Honeypots
- Sandbox Analysis
- SIEM



- Detecting cybersecurity *events*.
  - New devices or users
  - Recently installed software/applications
  - Failed logins
- Monitoring all the things, all the time.

# DETECT Categories

- Anomalies and Events: 5 subcategories
- Security Continuous Monitoring: 8 subcategories
- Detect Processes: 5 subcategories



# RESPOND

- Endpoint Threat Detection and Response (ETDR)
- Network Behavior Analysis
- GRC Tools
- Global Threat Feed Tools
- (SOC) + Automation

- Containing the impact of a cybersecurity incident.
- Responding to alerts created by the detection tools.
- People need to know their roles and responsibilities during an incident.
- Review responses retroactively and incorporate *lessons learned*.

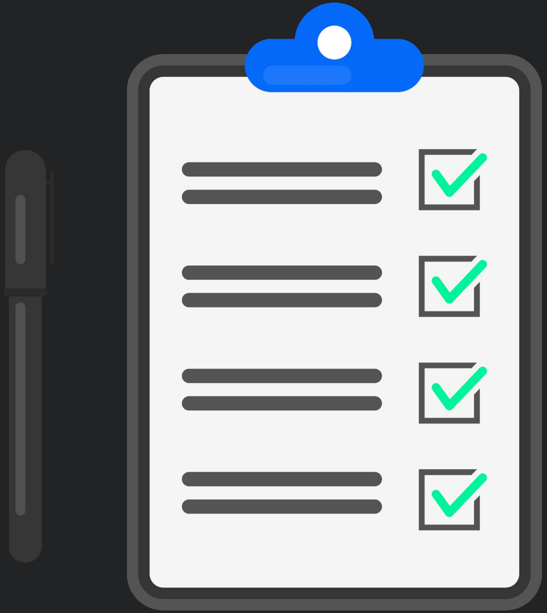
# RESPOND Categories

- Response Planning: 1 subcategory
- Communications: 5 subcategories
- Analysis: 5 subcategories
- Mitigation: 3 subcategories
- Improvements: 2 subcategories

# RECOVER

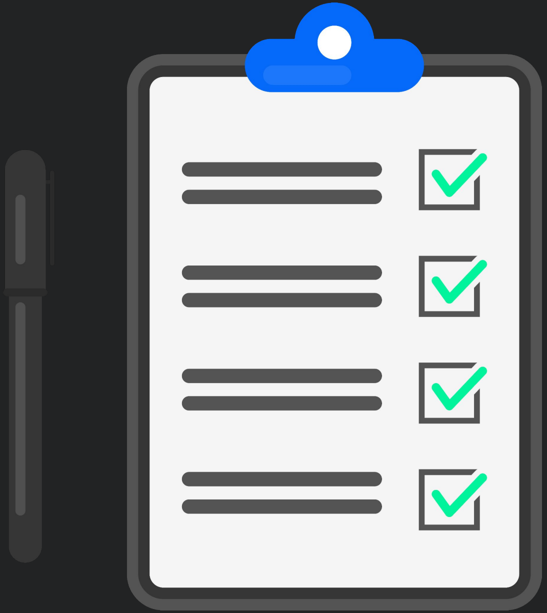
- Data replication and backup
- DR COOP Sites
- Disaster Recovery Plans

- Prioritize the data so you can restore based on business needs.
- Test your backups
- Tabletop exercises

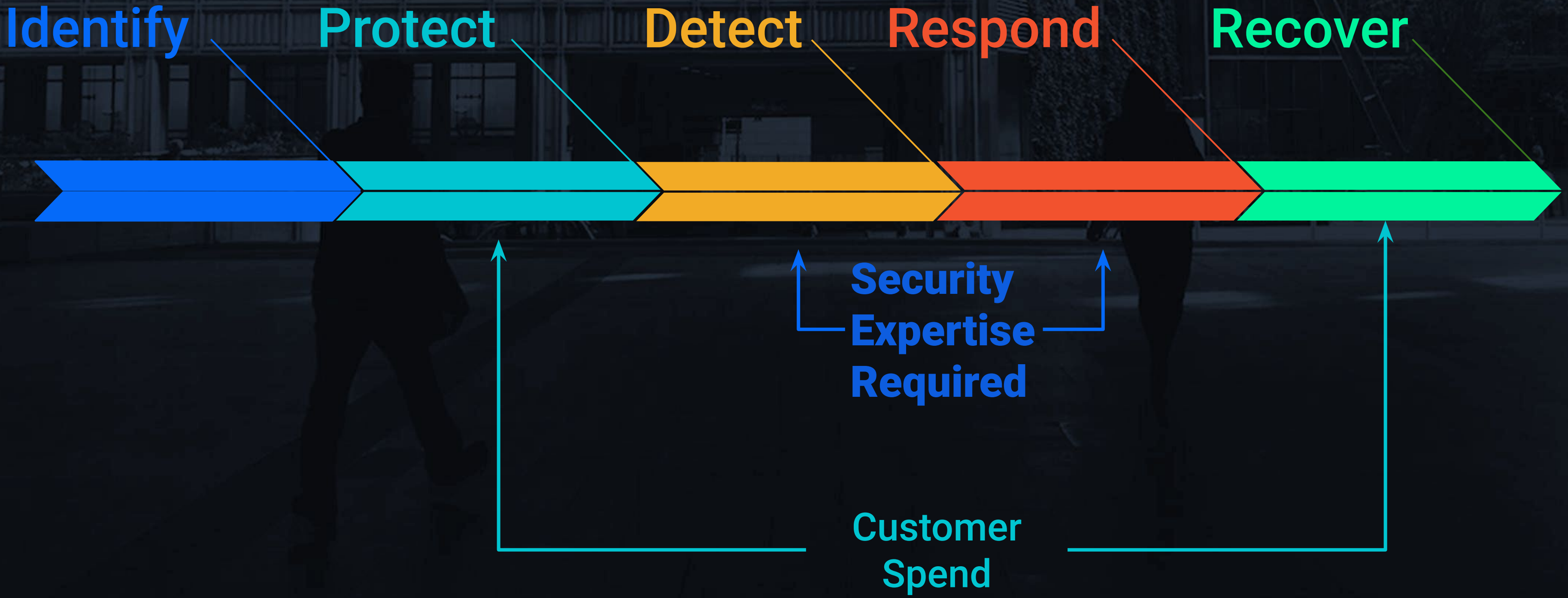


# RECOVER Categories

- Recovery Planning: 1 subcategory
- Improvements: 2 subcategories
- Communications: 3 subcategories



# NIST Cybersecurity Framework



Identify

Protect

Detect

Respond

Recover

Security Expertise Required

Customer Spend

# NIST Cybersecurity Framework

## Identify

- Asset & Network Mgmt
- Governance, Risk, Compliance
- Vulnerability Management

## Protect

- AV/NGAV
- Firewalls
- DNS Filtering
- NAC / MFA
- Email Filtering
- Phishing Training
- Encryption
- IPS

## Detect

- Threat Hunting
- Endpoint Threat Detection
- Network Behavior Analysis
- Honeypots
- Sandbox Analysis
- SIEM
- IDS

## Respond

- Endpoint Threat Detection and Response (ETDR)
- Network Behavior Analysis
- Global Threat Feed Tools
- (SOC) + Automation

## Recover

- Data replication and backup
- DR COOP Sites
- Disaster Recovery Plans
- Incident Response Plans
- Cyber Insurance

# Framework Profiles

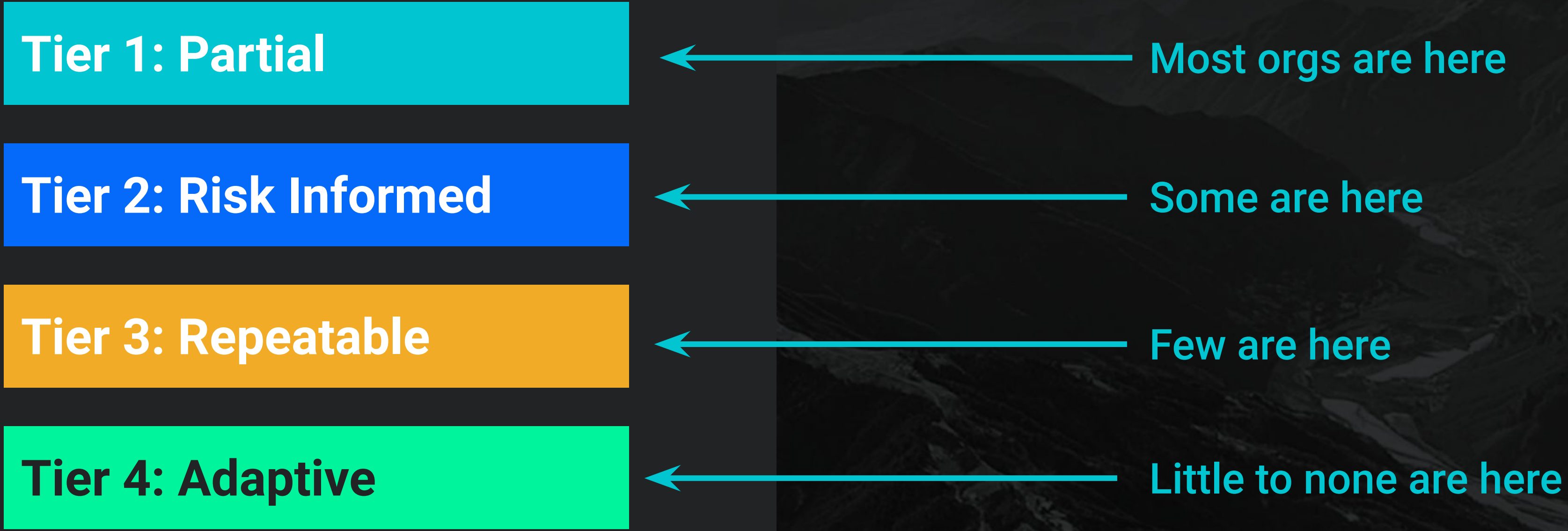
## Aligning the Framework Core With Organizational Goals

- Current Profile
  - Reflects the current state of the organization.
  - Requires periodic updates for target profile alignment.

- Target Profile
  - The agreed upon profile of the organization.
  - As business needs change, the target profile should be updated to reflect such changes.

- Profile Comparison
  - Helps identify gaps between the current and target profile.

# Implementation Tiers



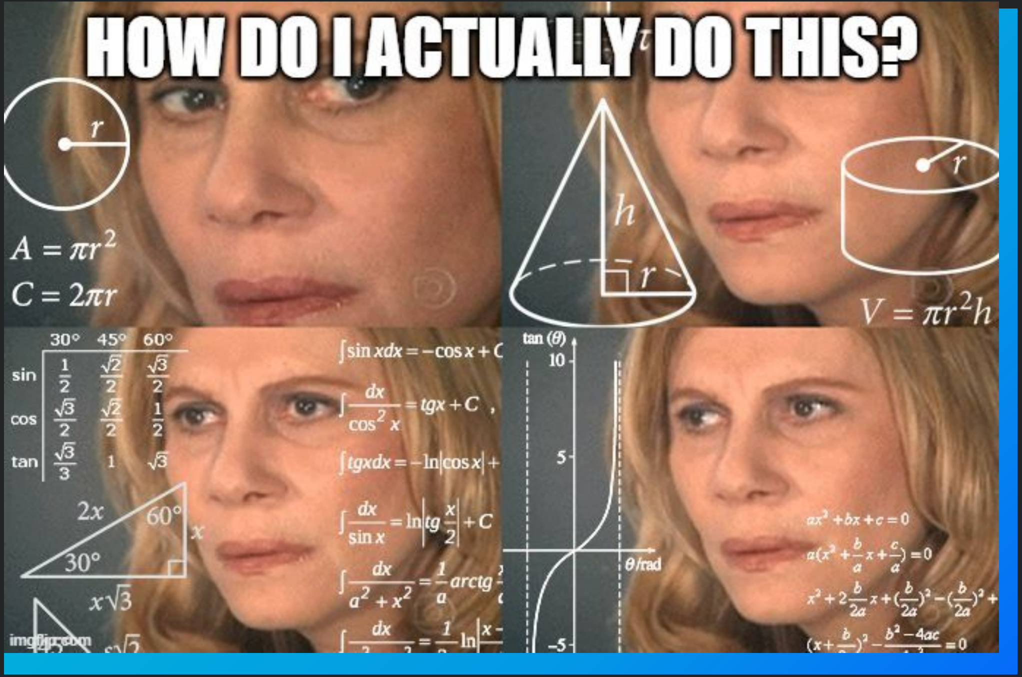
Tier 1: Partial ← Most orgs are here

Tier 2: Risk Informed ← Some are here

Tier 3: Repeatable ← Few are here

Tier 4: Adaptive ← Little to none are here

# There has to be a shortcut… or a simpler starting path, right?



# 03

# CIS Controls

# CIS Contols Enters the Chat

## Complementary to the NIST CSF

NIST CSF

- **Descriptive** in nature - “What good looks like across the board”
- Created by NIST (think: federal government)
- More holistic around people, process and technology

CIS Controls v8

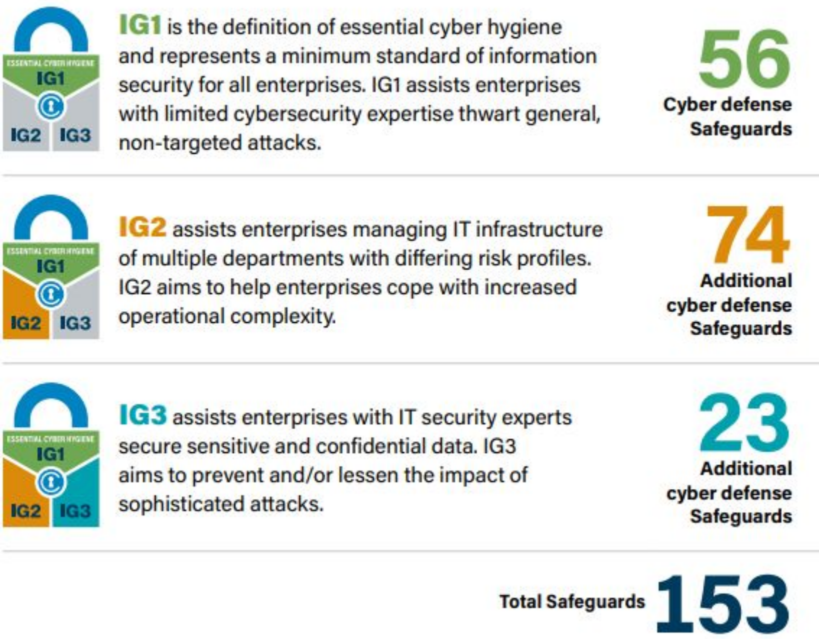
- **Prescriptive** in nature - “How-to”
- Created outside of government (SANS and now CIS)
- Mostly focused around identification and prevention

# CIS Controls v8

**18 Controls**

**3 Implementation Groups**

**153 Safeguards**


ESSENTIAL CYBER HYGIENE
IG1
IG2
IG3

**IG1** is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

**56** Cyber defense Safeguards

**IG2** assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

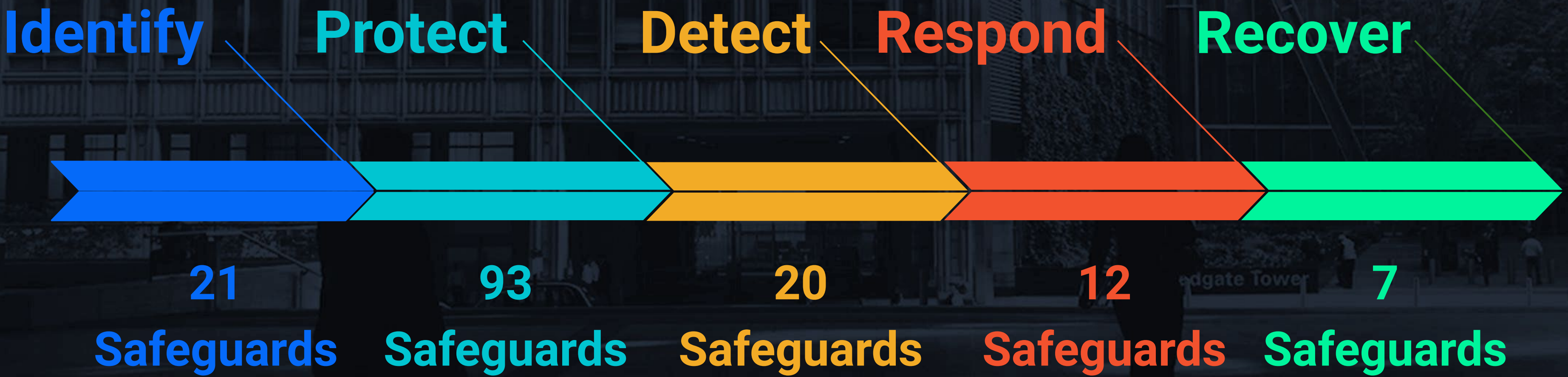
**74** Additional cyber defense Safeguards

**IG3** assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

**23** Additional cyber defense Safeguards

Total Safeguards **153**

# CIS Controls’ Safeguards



Identify

Protect

Detect

Respond

Recover

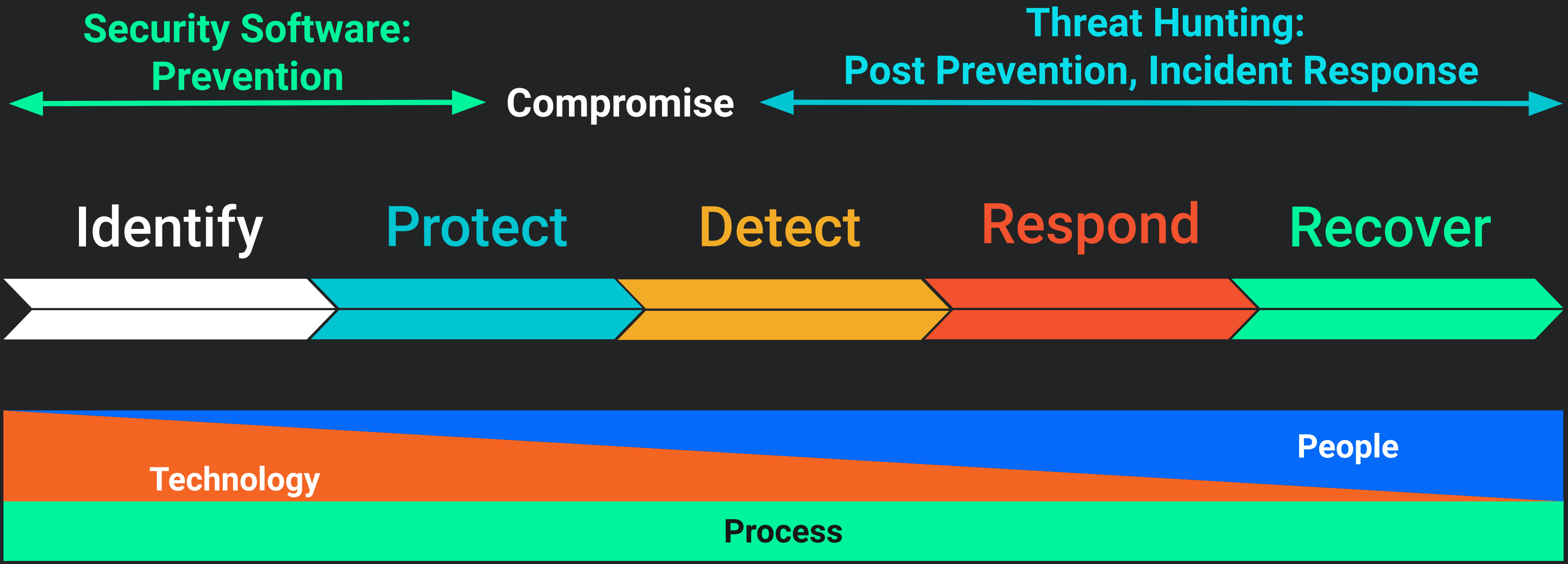
21 Safeguards

93 Safeguards

20 Safeguards

12 Safeguards

7 Safeguards



Security Software: Prevention

Compromise

Threat Hunting: Post Prevention, Incident Response

Identify

Protect

Detect

Respond

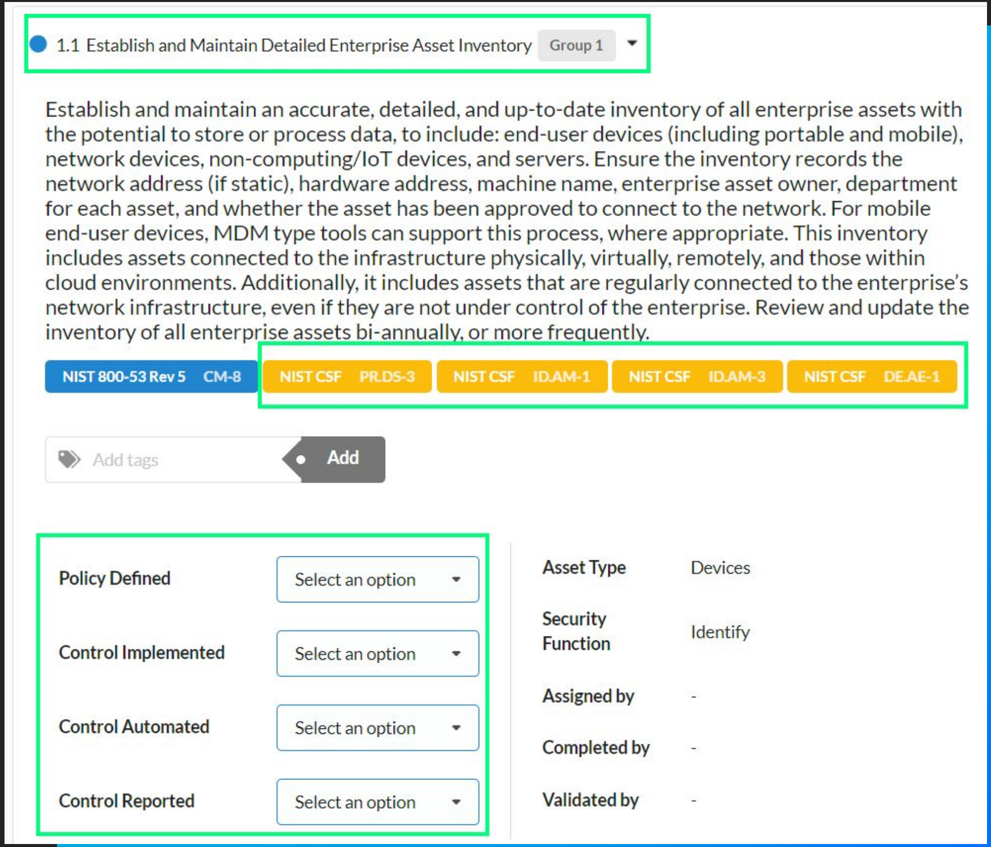
Recover

Degree of Dependency

https://www.nist.gov/cyberframework
https://www.cyberdefensematrix.com

# CIS CSAT

- The Controls Self Assessment Tool can help guide the implementation of your stack.
- Maps to NIST CSF subcategories.
- Can possibly be of use in your marketing.



● 1.1 Establish and Maintain Detailed Enterprise Asset Inventory Group 1

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

NIST 800-53 Rev 5 CM-8 | NIST CSF PR.DS-3 | NIST CSF ID.AM-1 | NIST CSF ID.AM-3 | NIST CSF DE.AE-1

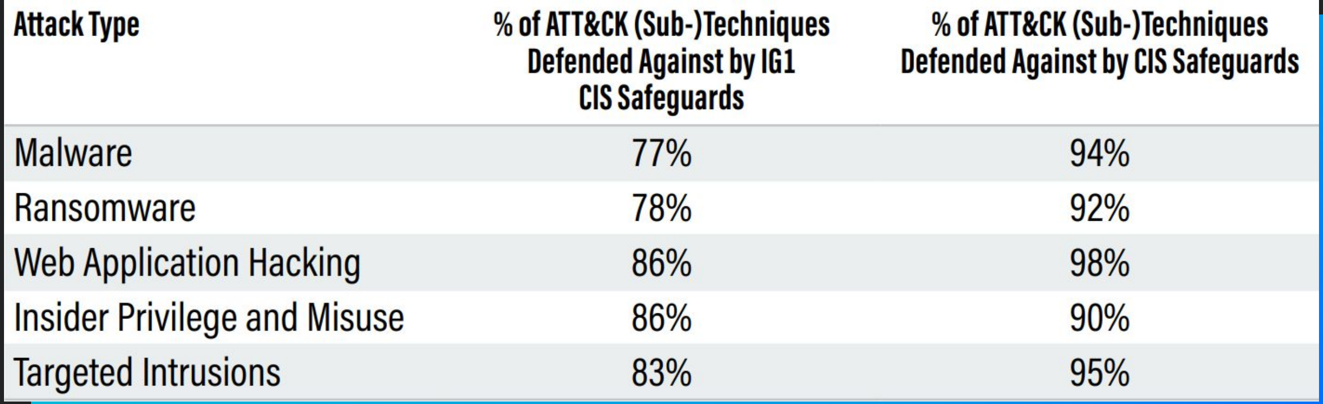
| | |
|---|---|
| Policy Defined | Select an option |
| Control Implemented | Select an option |
| Control Automated | Select an option |
| Control Reported | Select an option |

| | |
|---|---|
| Asset Type | Devices |
| Security Function | Identify |
| Assigned by | - |
| Completed by | - |
| Validated by | - |

> Enterprises achieve a high level of protection and are well-positioned to defend against the top five attack types through implementation of essential cyber hygiene, or IG1. -CIS

Center for Internet Security (CIS) Releases New Community Defense Model for Cybersecurity (cisecurity.org)

# IG1 Coverage across the Top 5 Attack Types



| Attack Type | % of ATT&CK (Sub-)Techniques Defended Against by IG1 CIS Safeguards | % of ATT&CK (Sub-)Techniques Defended Against by CIS Safeguards |
|---|---|---|
| Malware | 77% | 94% |
| Ransomware | 78% | 92% |
| Web Application Hacking | 86% | 98% |
| Insider Privilege and Misuse | 86% | 90% |
| Targeted Intrusions | 83% | 95% |

# 04

# Takeaways

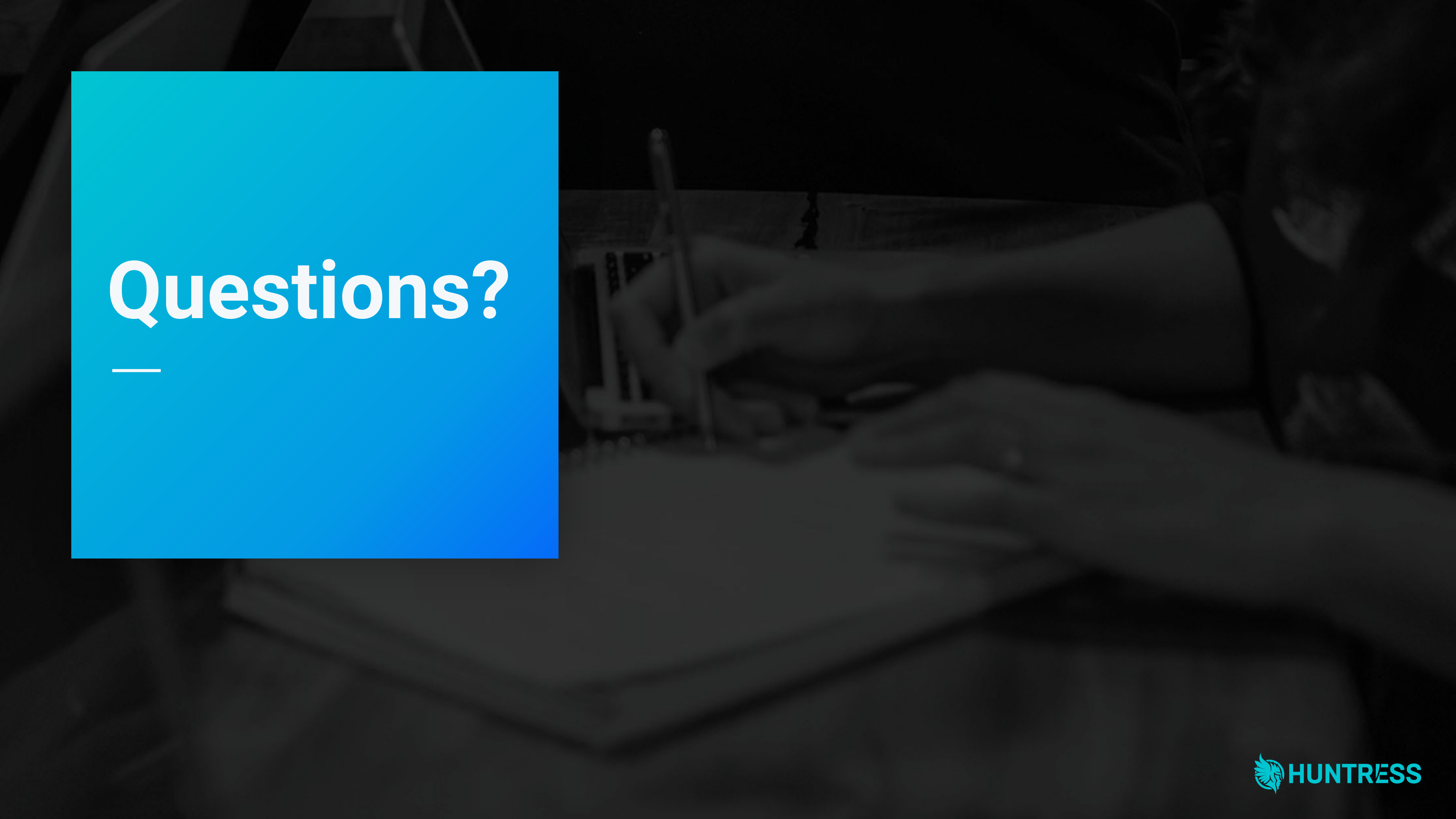
# Takeaways

- You MUST start somewhere!
  - We love CIS as a starting point.
  - IG1 is a starting point
  - CSF is perfect as you mature past CIS IG1 and as a guide to “learn more”

- Assess your current controls. Where are your gaps?
  - CSF and CIS should drive your tool adoption

- Security frameworks are your BLUEPRINT for security success.

- Stop selling tools and start selling expertise.



# Questions?

# Thank you

# Test-Drive the Platform

## Start your free 21-day trial today

- Deploy in minutes to an unlimited number of endpoints
- Remediate persistent footholds and other identified threats
- Receive custom incident reports From our ThreatOps team

HUNTRESS

huntress.com/trial

HUNTRESS