HIMSS Cybersecurity Community Sponsor

Security Fundamentals

based on the NIST Cybersecurity Framework

Speaker Introduction

Rick Spatafore

CPHIMS, GISP, GCIH, HCISPP

Manager, Advisory Services with Sentinel Technologies

15 years Healthcare IT

15 years cybersecurity & compliance

25 years in technology


What are cybersecurity fundamentals?

Security Data & Research

enterprise.comodo.com › blog › what-is-next-gen-endpoint-protection

What is next-gen endpoint protection? Ways to Secure Your ...

Jan 14, 2018 - Next-gen **endpoint protection** means looking behind vendor claims. Learn the elements that make endpoint security truly **next generation**.

www.sophos.com › en-us › endpoint5reasons

Next-Gen Endpoint Protection: Switch to Sophos Today | On ...

Sophos **Next**-Gen **Endpoint Protection** integrates innovative security technologies to protect against all stages of an attack, coordinated through a central control ...

www.cisco.com › Products & Services › Security

Endpoint Security - Cisco Next-Generation Endpoint Security

Threats have evolved. Your **endpoint protection** solution should, too. Cisco offers **next-generation** endpoint security through a combination of cloud- and ...

www.sentinelone.com › blog › what-is-next-generation-endpoint-prot...

What is Next Generation Endpoint Protection? | SentinelOne ...

May 20, 2015 - By now you have probably heard the term "**Next Generation Endpoint Protection**. A slew of companies, startups and incumbents alike use the ...

blog.avast.com › the-next-generation-of-endpoint-security

The Next Generation of Endpoint Security | Avast Business

Oct 5, 2019 - Large companies have IT departments to deploy **next-generation endpoint protection**, but as the owner of a small business, it may fall to you to ...

Next-generation firewall

A next-generation firewall is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection, an intrusion prevention system. Wikipedia

Security Posture

Attacks are on the rise (2017, 2018, 2019)

- 2017-2018 included a small increase in breaches
- Data exposed tripled year over year

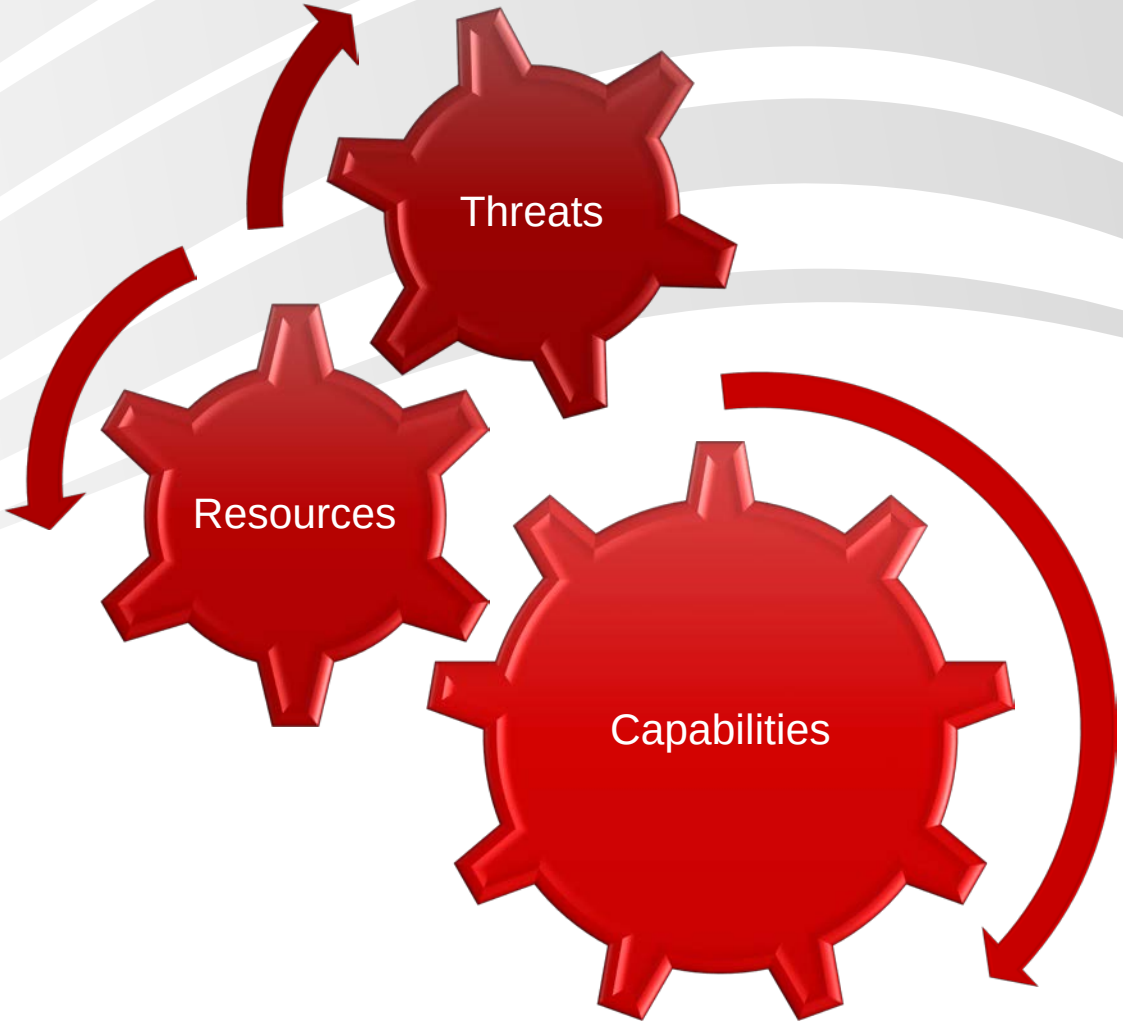
Ransomware will continue

AI was one of the top predictions for 2019

- AI is again a top prediction for 2020

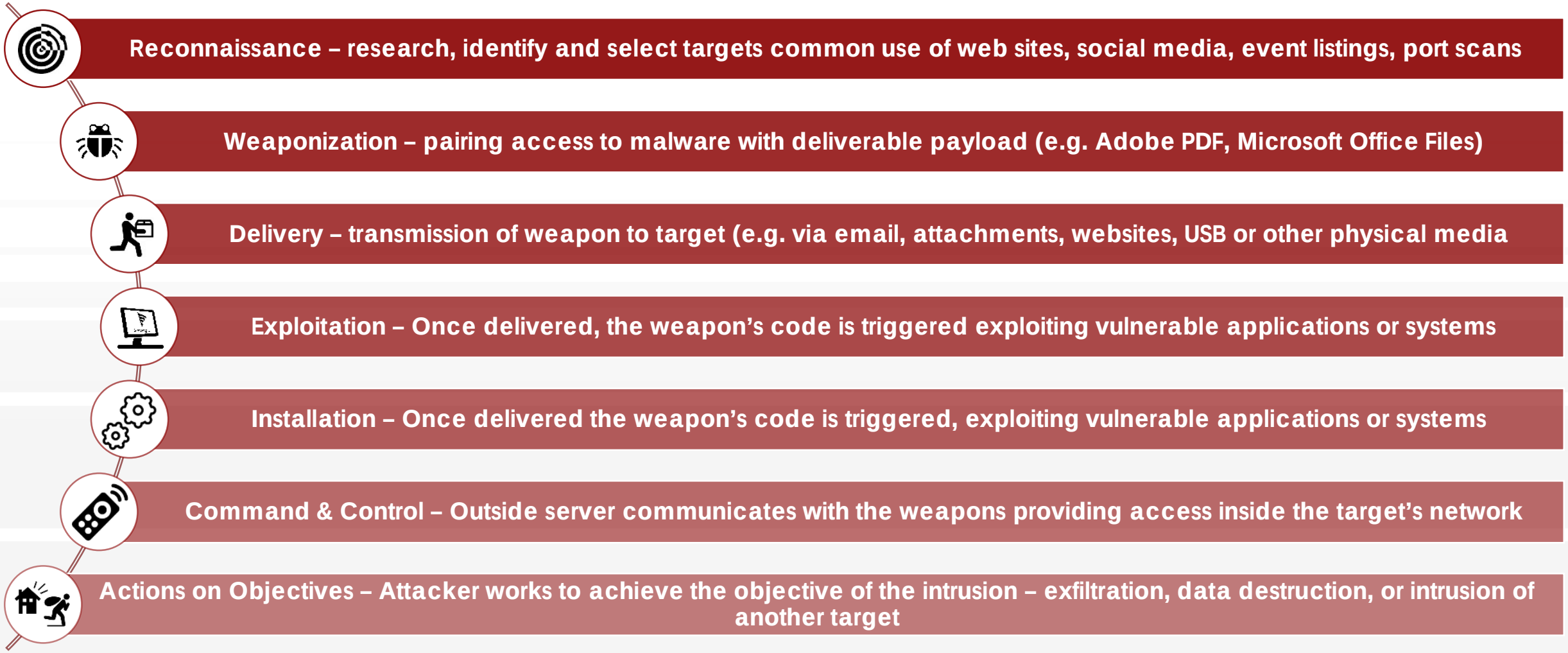
Cloud migration will increase security risk

Cloud security is not mature

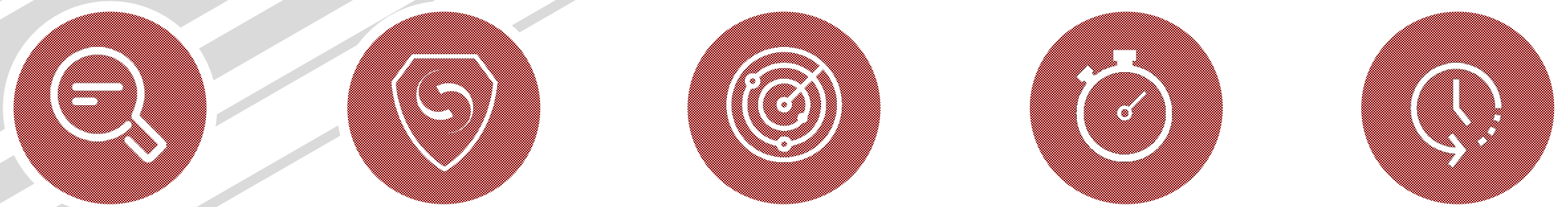


Security is not one size fits all

Cyber Kill Chain - Anatomy of an Attack



NIST Cyber Security Framework



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Identity Management	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Access Control	Security Continuous	Communications	Improvements
Governance	Awareness & Training	Monitoring	Analysis	Communications
Risk Assessment	Data Security	Detection Process	Mitigation	
Risk Management	Process & Procedures		Improvements	
Supply Chain Risk Management	Maintenance			
	Protective Technology			

NIST CSF: Identify

	Identify
	Asset Management
ID.AM-1	**ID.AM-1**: Physical devices and systems within the organization are inventoried
ID.AM-2	**ID.AM-2:** Software platforms and applications within the organization are inventoried
ID.AM-3	**ID.AM-3**: Organizational communication and data flows are mapped

NIST CSF: Identify

	Risk Assessment
ID.RA-1	**ID.RA-1:** Asset vulnerabilities are identified and documented
ID.RA-2	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources
ID.RA-3	**ID.RA-3:** Threats, both internal and external, are identified and documented
ID.RA-4	**ID.RA-4:** Potential business impacts and likelihoods are identified
ID.RA-5	**ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
ID.RA-6	**ID.RA-6:** Risk responses are identified and prioritized
	Risk Management Strategy
ID.RM-1	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders
ID.RM-2	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed
ID.RM-3	**ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

NIST CSF: Protect

	Protect
	Identity Management, Authentication and Access Control
PR.AC-1	**PR.AC-1:** Identities and credentials are managed for authorized devices and users
PR.AC-4	**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties
PR.AC-7	**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) (1.1)

SP 800-63-3
Digital Identity Guidelines

SP 800-63A
Enrollment & Identity Proofing

SP 800-63B
Authentication & Lifecycle Management

SP 800-63C
Federation & Assertion

Password: x

It would take a computer about

7 HUNDRED PICOSECONDS

to crack your password

Password: Locu$t0%

It would take a computer about

9 HOURS

to crack your password

Passphrase: I like to vacation in Hawaii!

It would take a computer about

100 UNDECILLION YEARS

to crack your password

NIST CSF: Protect

	Awareness & Training
PR.AT-1	**PR.AT-1:** All users are informed and trained
PR.AT-2	**PR.AT-2:** Privileged users understand roles & responsibilities
PR.AT-3	**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
PR.AT-4	**PR.AT-4:** Senior executives understand roles & responsibilities
PR.AT-5	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities

NIST CSF: Protect

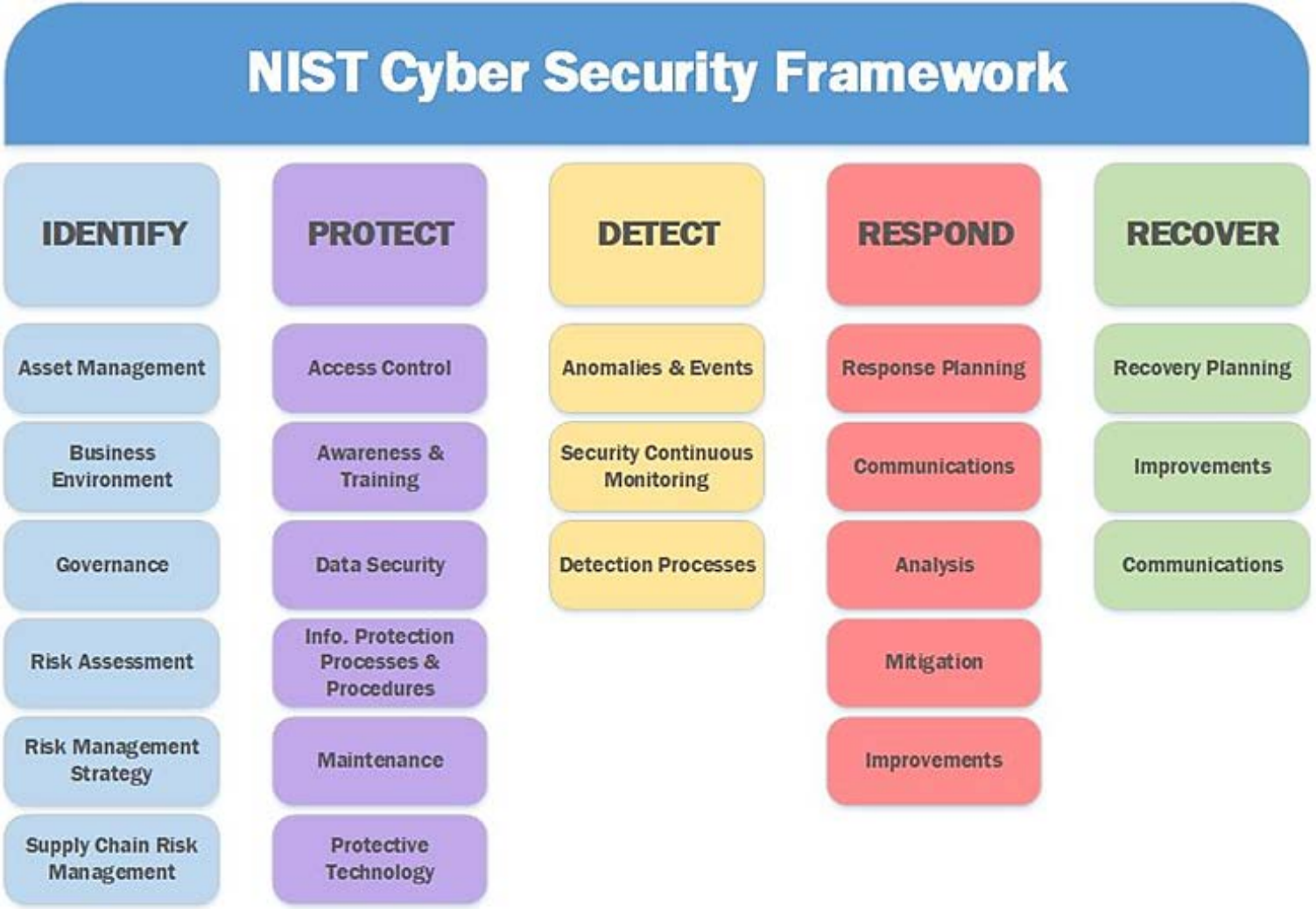
	Information Protection, Processes & Procedures
PR.IP-1	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained (e.g. concept of least functionality)
PR.IP-2	**PR.IP-2:** A System Development Life Cycle to manage systems is implemented
PR.IP-12	**PR.IP-12:** A vulnerability management plan is developed and implemented
PR.PT-3	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities (1.1)

NIST CSF: Protect & Detect

	Protect
	Information Protection, Processes & Procedures
PR.IP-12	**PR.IP-12:** A vulnerability management plan is developed and implemented

	Detect
	Security Continuous Monitoring
DE.CM-8	**DE.CM-8:** Vulnerability scans are performed

NIST Cybersecurity Framework



Q&A

Contact Information:

Rick Spatafore
Manager, Advisory Services
Sentinel Technologies
Office: 630.786.8062
rspatafore@sentinel.com