Man and Machine: Forming a Perfect Union to Mature Security Programs

Keynote Address

Global Cyber Security in Healthcare & Pharma Summit

London, UK

Innocent "Inno" Eroraha, CISSP-ISSAP, ISSMP, CISM, CISA, CHFI, CCSA, CCSE
Founder & Chief Scientist
NetSecurity Corporation
Dulles, Virginia, USA

February 6, 2020

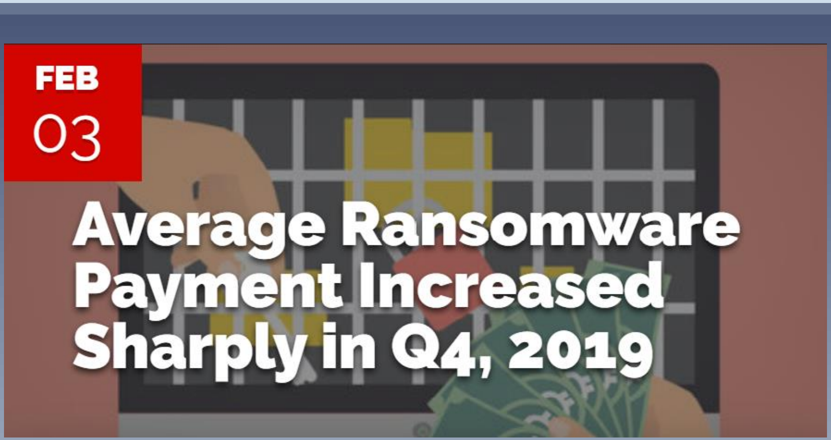
Data Compromised

Medical (72%), Personal (34%), Credentials (25%) (breaches)

HEALTH IT, MEDCITY INFLUENCERS

Why healthcare providers are losing the cybersecurity battle

It is time for medical organizations to re-assess the potential consequences of complacency, and equip their security teams with the resources they need to keep their staff, and ultimately their patients safe.



FEB 03

Average Ransomware Payment Increased Sharply in Q4, 2019

JAN 24

Critical 'MDHex' Vulnerabilities Identified in GE Healthcare Patient Monitoring Products

OCT 18, 2018

Ransomware News: WannaCry Costs NHS Over $100 Million Attack

BY CHRIS BRUNAU

. 15% of breaches involved Healthcare organizations, 10% in the Financial industry and 16% in the Public Sector. (Verizon)

URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication

Data breaches exposed **4.1 BILLION** records in the first half of 2019.

RiskBased

VARONIS

Man and Machine: Forming a Perfect Union to Mature Security Programs

Who is Hacking Your Network?

- First incident response encounter —What has changed since 1996
- Typical responses from CxOs regarding their perceived state of their security
- Unless you are situationally aware, you may be blinded to clandestine hacking activities
- Situationally aware organizations
  - Predict each employee's departure
  - Gain insight into insider threats and external attacks
  - Account for data leaving their organization
  - Are proactive instead of reactive

How prepared are you in preventing a breach?

Data Protection Challenges

- Explosion of technology and ubiquity of data
- The disintegrating perimeter
- Increase in attack surfaces in
  - Medically connected devices, enterprise mobility
  - Web apps, mobile devices, IoT devices, BYOT, cloud, etc.
  - Software bugs and vulnerabilities
  - Physical, facility, and personnel security
- Inadequate skilled personnel to tackle the cyber security problem
- Man and machine must work together to be ahead of the adversaries

The Threat Landscape

- Threat Actors
  - Innovative, relentless, and highly sophisticated
  - Nation-State, Lone Attackers, Organized Criminals
  - Competitors
  - Insiders
  - Partners (Supply Chain)
- Data Breach Vectors
  - Email, web, removable devices, file/network shares
- Defenses
  - What defenses exist to prevent successful breaches?
  - How well are defenses working?
  - How mature are existing processes or security program?

Disrupting the Status Quo

- Security culture must adapt to current challenges
- Less reliance on external audit to determine a clean bill of security health
- Going beyond pen testing
  - Breach/compromise assessment, threat hunting, etc.
- Leveraging people, process, and technology to innovate and automate
- Adapting a Security Framework to mature a security program

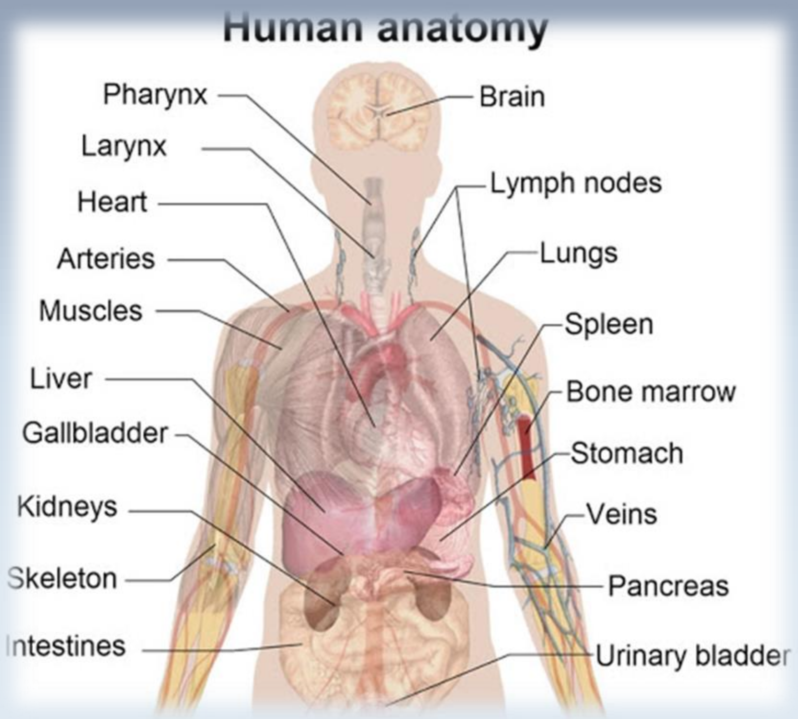
Do/Think Differently

- Gaining Domain Admin is not necessarily the most damaging compromise – other vectors may result in consequential damages
  - An adversary who is able to calibrate a medical device hooked up to a terminally ill patient
  - An attacker that is able to physically breach a hospital ward
  - A hacker that has gained access to publicly accessible S3 buckets
- Think like an adversary – without being one!
- Filter out the marketing hype and security buzzwords
  - ML, AI, Analytics, SAOR, Threat Hunting, etc.
- Get your entire team (NOT just IT/Security) security-aware
- **“Compliance/Certification ≠ Security”**
- Let auditors speak truth to power, without repercussion

Dig Deeper

- Complement penetration testing with
  - Breach/Compromise Assessments
  - Threat Hunting
- Account for each asset in the infrastructure stack in
  - Contingency Planning
  - IT Operations
  - Risk Assessment
- Go beyond the Operating System (OS)
  - **Patch management:** patch all assets, not just the OS
  - **Threat monitoring:** monitor all assets, not just OS
- Most assets often ignored in logging/protection
  - APIs, mobile devices, mobile apps, IoT devices, applications, databases, specialized equipment
- Be attentive to physical, facility, and personnel security

Securing the Enterprise is Like Protecting the Human Body



- Each organ ("asset") of the body ("enterprise") needs to be protected and in optimal state

Silver Bullet

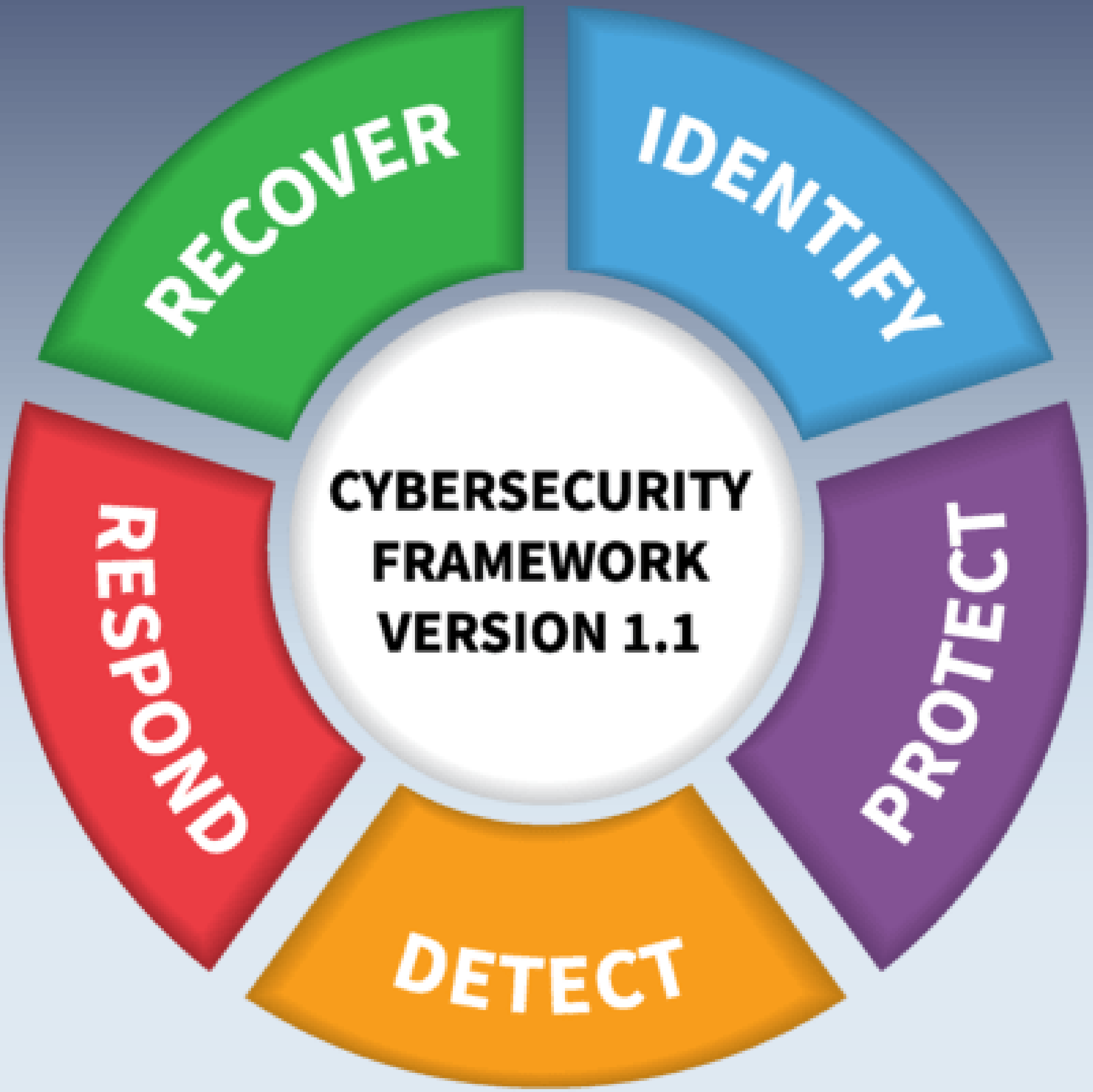
- There is no single solution that will detect and prevent attacks 100% of the time
  - Not Firewalls, EDRs, DLPs, UBAs, AVs – None!
  - *Run if any technology claims otherwise!*
- Existing technologies need to interoperate and scale

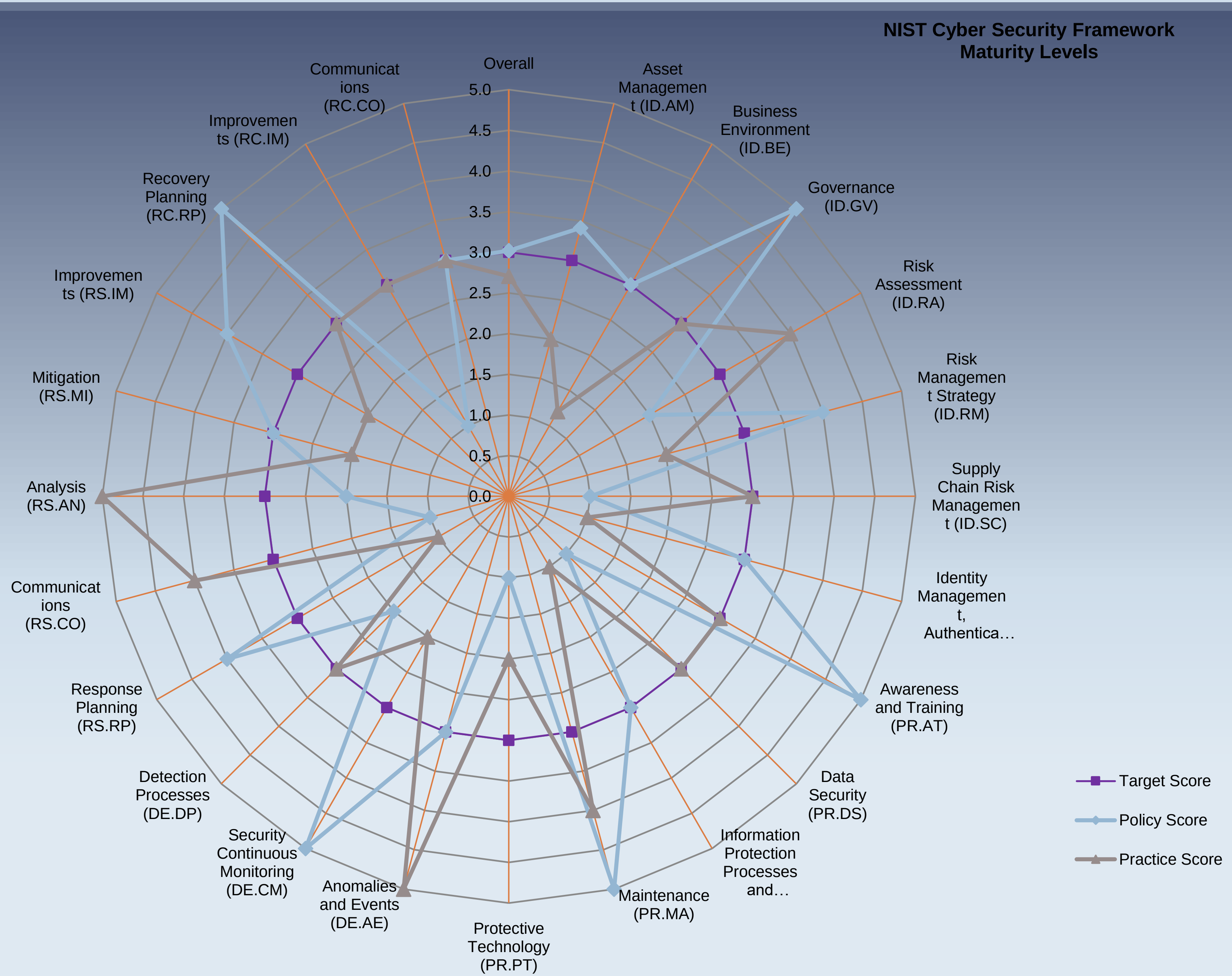
Know Your Assets and Risks

- □ Address the **who, what, where, why, when,** and **how** relating to each asset
- □ How would you know you are under attack?
- □ What and where are your assets?
- □ What are the "Vital Signs" of each asset?
- □ What are your attack surfaces?
- □ What are your data ex-filtration vectors?
- □ What are your vulnerabilities, threats, and likelihood?
- □ What are the risks of each assets?
- □ How are your facilities and personnel protected?

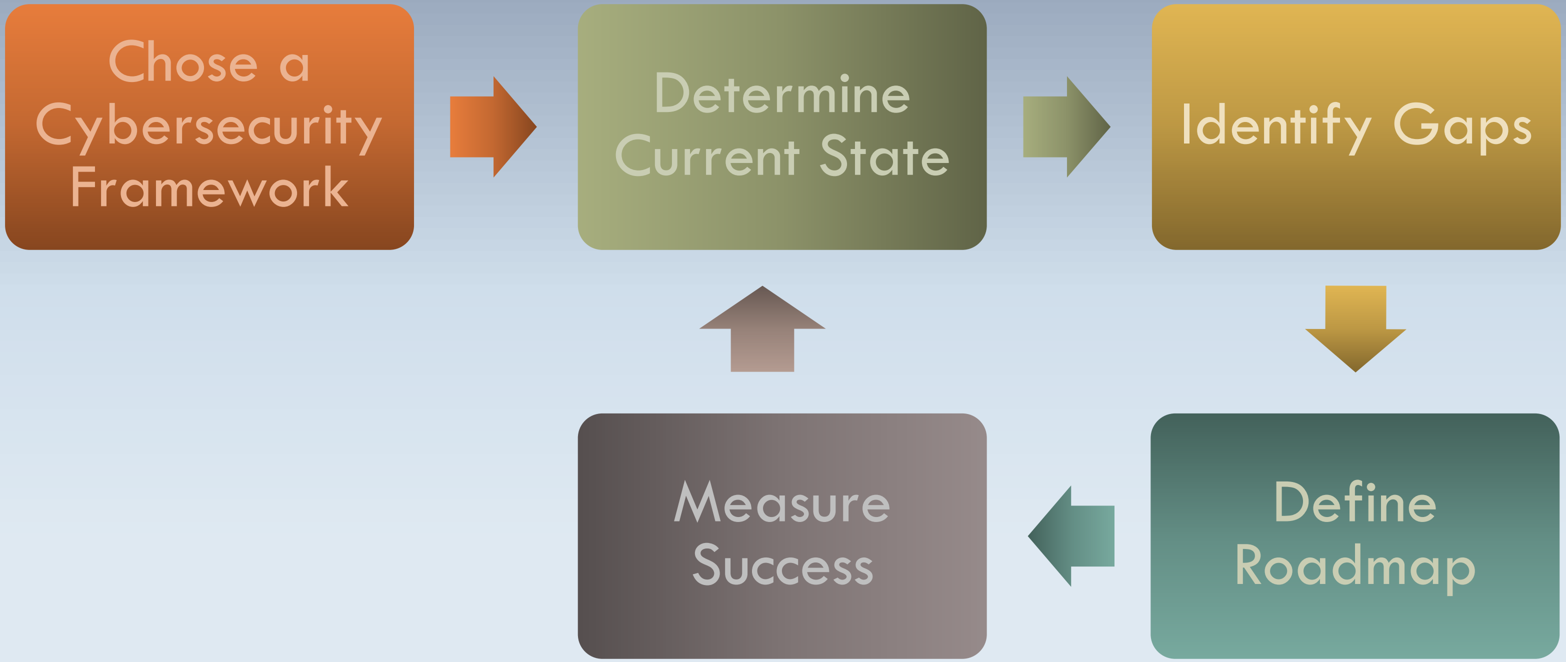
Cyber Security Maturity Model (CSMM)

- A CSMM enables an organization to compare its security program against predetermined benchmarks
- It answers questions relating to the program such as:
  - What is the current security state?
  - Where does the organization need to go?
  - What is the organization doing well in?
  - What areas does the organization need to improve upon?
- Using a framework helps:
  - Change culture
  - Improve communication and understanding around cybersecurity
- **Examples:**
  - NIST Cyber Security Framework (CSF)
  - Cybersecurity Capability Maturity Model (C2M2)


CYBERSECURITY FRAMEWORK VERSION 1.1
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER


NIST Cyber Security Framework
Maturity Levels
Overall
Asset Management (ID.AM)
Business Environment (ID.BE)
Governance (ID.GV)
Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM)
Supply Chain Risk Management (ID.SC)
Identity Management, Authentica…
Awareness and Training (PR.AT)
Data Security (PR.DS)
Information Protection Processes and…
Maintenance (PR.MA)
Protective Technology (PR.PT)
Anomalies and Events (DE.AE)
Security Continuous Monitoring (DE.CM)
Detection Processes (DE.DP)
Response Planning (RS.RP)
Communications (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)
Recovery Planning (RC.RP)
Improvements (RC.IM)
Communications (RC.CO)
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Target Score
Policy Score
Practice Score

Instituting a Cybersecurity Program



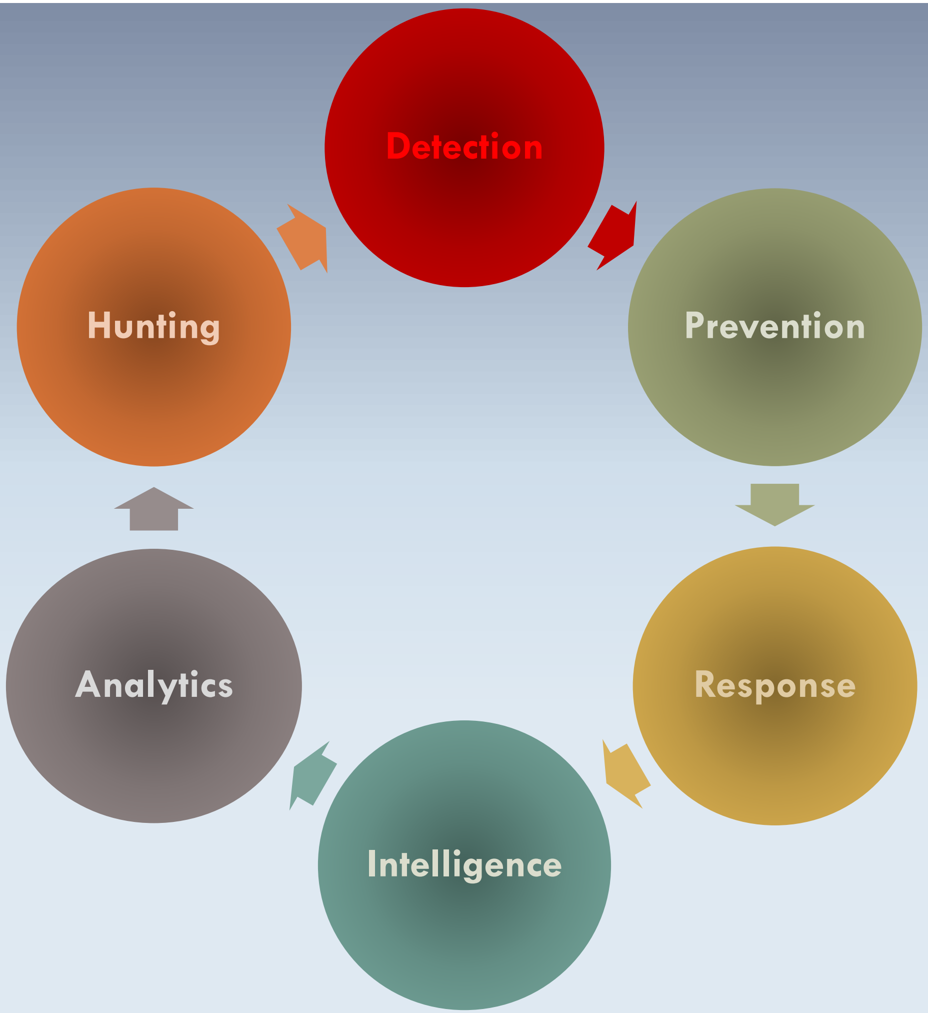
Building a Breach Response Capability

- Perform asset identification, data collection, and analytics
- Identify tools for risk, vulnerability, and threat management
- Retain trained and skilled personnel (internal and external)
- Develop processes – Incident Response Plan, Data Breach Response Plan, Procedures, etc.
- Proactively test and assess the Capability

Maturing a Cybersecurity Program

- Gaining situational awareness of:
  - Entire infrastructure stack and technology connected devices, medical devices, computing infrastructure, wireless devices, IoTs, BYOD, cloud, etc.
  - Physical, facilities, and personnel security
- Continuous monitoring (of controls)
- Build a culture-based security awareness training program
- Hold everyone accountable to security
  - Tie contracts and employee performance to security
- Establish a **Matured Threat Operation**

Automating Matured Threat Operation



Summary

- Securing the enterprise is like protecting the human body
- Complement Penetration Testing with Compromise Assessment and/or Threat Hunting
- Be situationally aware and avoid being blinded by adversarial activities
- Compliance **IS NOT** Security
- Know ALL your assets and risks faced by each
- Establish a Data Breach Response Capability now
- Create a Matured Security Program and measure success frequently
- Leverage machines and automation to mature your Security Program

References

- □ https://www-businessinsider-com.cdn.ampproject.org/c/s/www.businessinsider.com/why-humans-not-machines-are-companies-biggest-competitive-advantage-2020-1?amp
- □ http://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce
- □ https://www.varonis.com/blog/cybersecurity-statistics/
- □ https://johnmasserini.com/2019/01/28/free-nist-csf-maturity-tool/
- □ https://enterprise.verizon.com/en-gb/resources/reports/dbir/2019/healthcare/