State of Alaska
Department of Administration

State of Alaska Cyber Security

Presentation to Senate State Affairs

Bill Smith, Office of Information Technology

1/20/2022

Agenda

Current Global Climate of Security

State's Cyber Security Posture

- **Current Capabilities**
- **Enhancements**

Path forward

Current Global Security Climate

Threat activity drivers:

- Cybercrime is a $6 trillion annual industry[1]
- Industrialization and automation of cyberattack capabilities
- Nation state threats
- Supply chain activity
- Pre-existing vulnerabilities

Breaches are no longer just a technical problem best handled by technical people, but instead threat awareness is the responsibility of the whole organization.[2]

Current Capabilities

- **Enterprise Security Solutions to eliminate legacy gaps in coverage**
  - Modernized productivity applications with rapid updates and increased security
  - Significantly expanded our ability to see attackers in real time
  - Expanded Endpoint Detection and Response across the executive branch
  - Upgraded Email Filtering and Spam Detection

- **Key Security Initiatives**
  - Elevated licensing for State of Alaska employees to increase security features (CRF)
  - Conducted comprehensive, detailed network inspection (20K+ devices)
  - Conducted external scanning to identify and address external facing vulnerabilities

- **Established intelligence and response collaboration (MS-ISAC, CISA)**
  - Strengthened existing partner relations with CISA, FBI, and AKNG
  - Expanding partnerships by way of participation in the Joint Cyber Security Multistate Program and the Alaska Cyber Group

Enhancements

***National Institute of Standards and Technology (NIST) Cybersecurity Framework*[4]**

Identify

- Asset Management
- Implementation of Multi-Factor Authentication (MFA)

Protect

- Continued hardening of the environment
- Migration to a secure Cloud Framework
- Recurrent Security Training for all state employees

Detect

- Network threat visibility - ability to detect real-time attacks and block malware, phishing attempts

Respond

- Security mentor led incident response rehearsals to improve readiness

Path forward – Focus on the basics

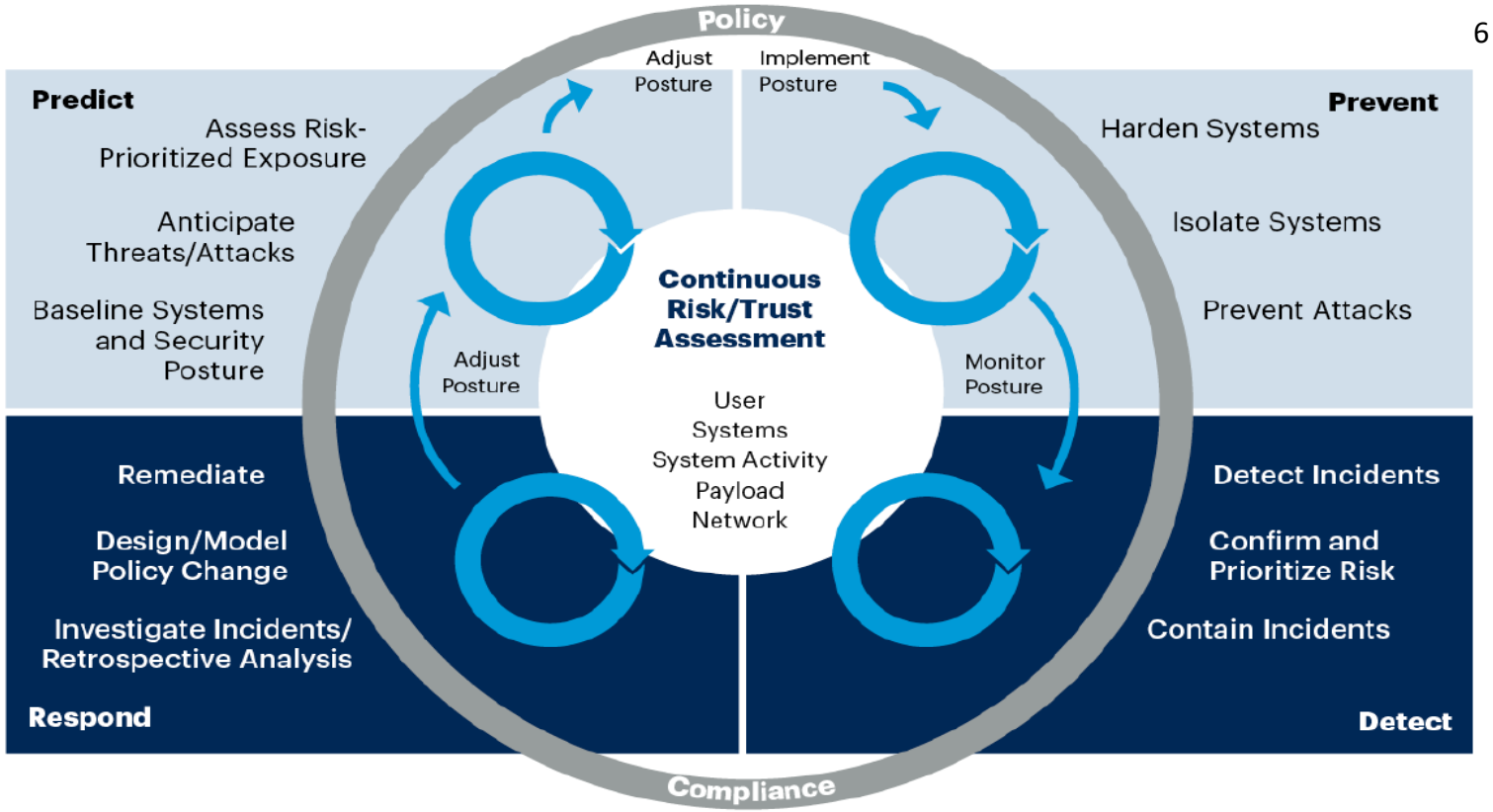
Focus on executing basic protocols well

- Practicing Good Cyber Hygiene[5]
- Compliance monitoring
- Enhance response capabilities
- Immediate threat hunting protection against security threats

Path forward – A holistic view

Simplify the enterprise security environment

- Developing a holistic view of security that is:
  - Integrated
  - Standardized
  - Working towards continuous improvement



Source: Gartner

719273_C

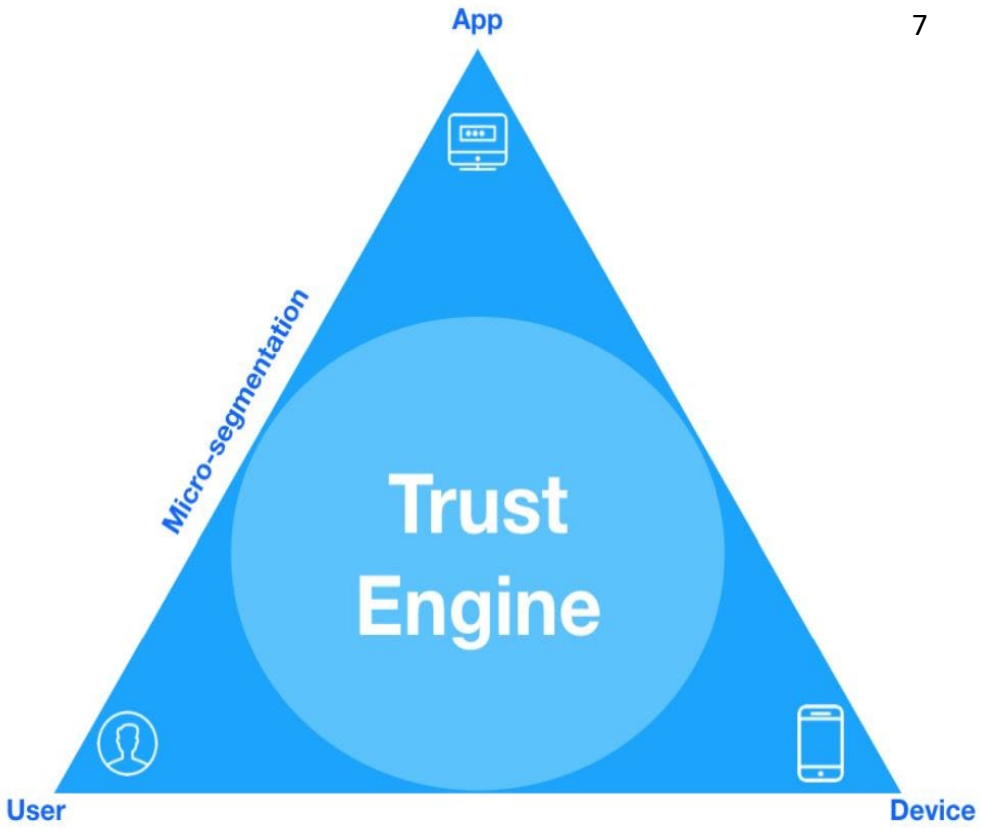
Gartner

Path forward – Zero Trust

Continue the path to Zero Trust

- Assume breach
- Verify explicitly
- Least privileged access

"A zero trust cybersecurity approach removes the assumption of trust typically given to devices, subjects (i.e., the people and things that request information from resources), and networks…. This requires device health attestation, data-level protections, **a robust identity architecture**, and strategic micro-segmentation to create granular trust zones around an organization's digital resources." *National Cybersecurity Center of Excellence (NCCoE), NIST* **Zero Trust guiding principles**



Questions

Background Slides

CYBERSECURITY FRAMEWORK
Aligns to Gov't and Industry Standards

Capability	Description
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure protection of the enterprise's assets.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

References

1. Security Magazine. The new threat economy: A guide to cybercrime's transformation – and how to respond, Brown, L., 2021
2. Gartner, The Urgency to Treat Cybersecurity as a Business Decision, Proctor, P., 2021.
3. ENISA, Threat Landscape 2021, ENISA,2021
4. NIST Cybersecurity Framework, The Five Functions of the Cybersecurity framework. NIST.,2018.
5. Microsoft Digital Defense Report. Microsoft, 2021
6. Gartner, How to Respond to the 2020 Threat Landscape, Watts, J., 2020
7. Zero Trust Cybersecurity Current Trends, American Council for Technology, 2019

Department of Administration

Championing improvement in the State's performance and results.

For more information, please contact Kelly Hanke at kelly.hanke@alaska.gov