Adaptive Security – One CISO’s Journey

Gary Hayslip
VP, CISO - Webroot
ADAPTIVE SECURITY (AS) – A CISOS JOURNEY

INTRODUCTION

ADAPTIVE-SECURITY AS A PLATFORM
• FEDERAL GOVERNMENT
• MUNICIPAL
• PRIVATE INDUSTRY
Security Defined

**Security:** freedom from, or resilience against, potential harm from external forces.

**Cybersecurity:** techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

**Adaptive Security:** approach that has become more widely used in response to a rapidly changing threat environment. Goal is to create a feedback loop of threat visibility, detection, and prevention that consistently becomes more effective.
Federal Government – My Experience

01 20 years active duty, 7 years civil service

02 Numerous positions in IT and Cybersecurity

03 Networks of 100 to 5,000+ employees

03 Legacy, SIPR, NMCI, Exempted
Risk – it’s all Black and White

- Assessment
- Certification
- Verification
- LifeCycle

NIST rules here!

Checksheets for everything
Federal Government – NIST Rules the Day

01 Networks & processes must follow specific assessment methodologies

02 IT assets, applications, services are purchased from specific vendors lists

03 Cyber and IT operations focused on meeting NIST requirements not business needs

04 Changes to certified networks starts the assessment loop all over again

05 Extremely challenging to get new applications, services, hardware cleared for networks
Federal Government

Lessons in Futility – AS would not work

Risk Management – extremely rigid
Threat Space – extremely fluid
Five years lag time on technology
High Turnover of Personnel
Municipal Government – My Experience

01  4 years as Deputy IT Director and CISO

02  25 networks, 40,000+ endpoints

03  11,000 employees, 3.2 million citizens

03  Legacy infrastructure to massive smart city/IoT projects
Municipal Government – a Beginning

Building an integrated platform

- Inventory – what do I have?
- Budget – funds, grants, startups
- Partnering with cyber startup community
- Smart City – leveraging technology
- Open data and then some
SMART CITY NETWORKS UNIQUE USE CASE FOR ADAPTIVE SECURITY

- Data Center & IT Security
- Service Layer
  - SSC: Energy Monitoring, Resource Monitoring & Saving, Operational Support for EVs
- Network Layer
  - Carrier Network, IP Network
- Sensing Layer
  - Community: Electric Power, Energy, Homes, Water, Mobility, Logistics, Healthcare
  - Sensors: Connected to vehicles, Traffic, Street Lights, Meters, Water, Police
- Future Sensors
  - Future Sensors to be connected to department sub-segment for optimization of resources
Municipal – Smart City Challenges

ADAPTIVE SECURITY AS A PLATFORM CHALLENGES

- Legacy systems, non-traditional endpoints, IoT, BYOD
- Network traffic and various perimeters
- Vendors, outsourced IT and services, 3rd party connections
- Limited security budgets / staffing / skills / politics
- Log information and maintenance
Municipal Government

**Lessons Learned – AS would work in limited capacity**

- **Risk Management –** must establish and maintain
- **Threat Space –** extremely fluid, disparate technologies results in high risk
- **Will make changes quickly but funds and paperwork causes lag**
- **Hybrid would be best approach for critical services & infrastructure**
Private Industry – My Experience

01 18 months as VP and Global CISO

02 400k SMB’s, 14k+ MSPs as customers

03 700+ employees, International office footprint

03 AWS, Google, Azure cloud presence
Private Industry – Netflix F.I.D.O.
Scoring Engine
Assessing the Data

- Alert
- Threat Feeds
- Historical
- Data Source
- User Asset Machine
- User Asset Machine Threat Total
- Support Person

Correlation

Scoring 0%-100%
Private Industry – Today!

Adaptive Security – Let’s build it, Yes we can!

- Risk Management – assessment & baseline
- Strategic Plan – based on ISO and NIST
- Security Stack Review
- Personnel Skillset Review
Private Industry – Adaptive Security Platform

ADAPTIVE RESPONSE – LIFE-CYCLE of an ANOMOLOUS INCIDENT

Security Orchestration & Automation Platform

CORRELATION
- Detectors
- Previous Threats
- Threat Feeds
- Metrics
- Operating Systems
- Thresholds
- Configurations
- Attack Simulations
- Protectwise

SCORING
- Threat
- User
- Machine
- Asset
- Data Type
- Venaler
- Business Case

ENFORCEMENT
- KIP NIC
- Kill VPN
- Client Sandbox
- Network Sandbox
- Automated Re-Image
- DNS Blacklist
- Packet Capture
- EDR
- Network IPS

HOST DETECTION
- Anti-Virus
- EDR
- DNS Tool
- SSL
- RPC

THREAT STACK
- Virus Totty
- SpaceFire
- MS-ISAC
- IT-ISAC
- Threat Intelligence
- BrightCloud

DATA SOURCES
- Anti-Virus
- IPS
- Packet Capture
- Vulnerability
- Scanner
- Patch Management
- EDR
- Config
- Management
- DLP
- Network IPS

NOTIFICATION
- Recommend Action
- Link to Cases
- Actions Performed
- Change Ticket
- Incident Ticket
- SMS Entry (Archer)
- Email
- SMS
- Phone Tree

Filter Detector Data
Filter Detector Data

Log Files and Data from other Technology stacks

SIEM
“Traffic Cop”
Adaptive Security Platform – Core Technologies

- Host/Network Detectors
- Threat Feeds/Sources
- Data Sources
- Correlation Engine
- SIEM, Dashboards
- Notification Technologies
Lessons Learned – AS takes time but will work

- AS should be part of cyber hygiene efforts
- For AS to be successful align it to business operations
- For AS to be established as a program = demonstrate value
- AS needs to be aligned with AI/ML through us of Orchestration & Automation
Thank you!

Questions?