Evolving the Security Strategy for Growth

Eric Schlesinger

Global Director and CISO

Polaris Alpha

Evolving the Security Strategy for Growth

POLARIS ALPHA

Where Do We Start?

Our History, Making History

- In late 2016, three companies merged together with the shared vision of creating a highly technical, mid-sized, premier solutions provider to the national security industry.

- Each was chosen for their outstanding contributions to the defense and intelligence environment—**EOIR** with state-of-the-art smart sensing, video analytics, and electromagnetic warfare efforts; **ISS** with data analytics, space command and control, and mission planning capabilities; and **Proteus Technologies** with advanced cybersecurity services.

- Throughout 2017, three other companies were added for their expertise and experience with providing advanced cyber mission support.

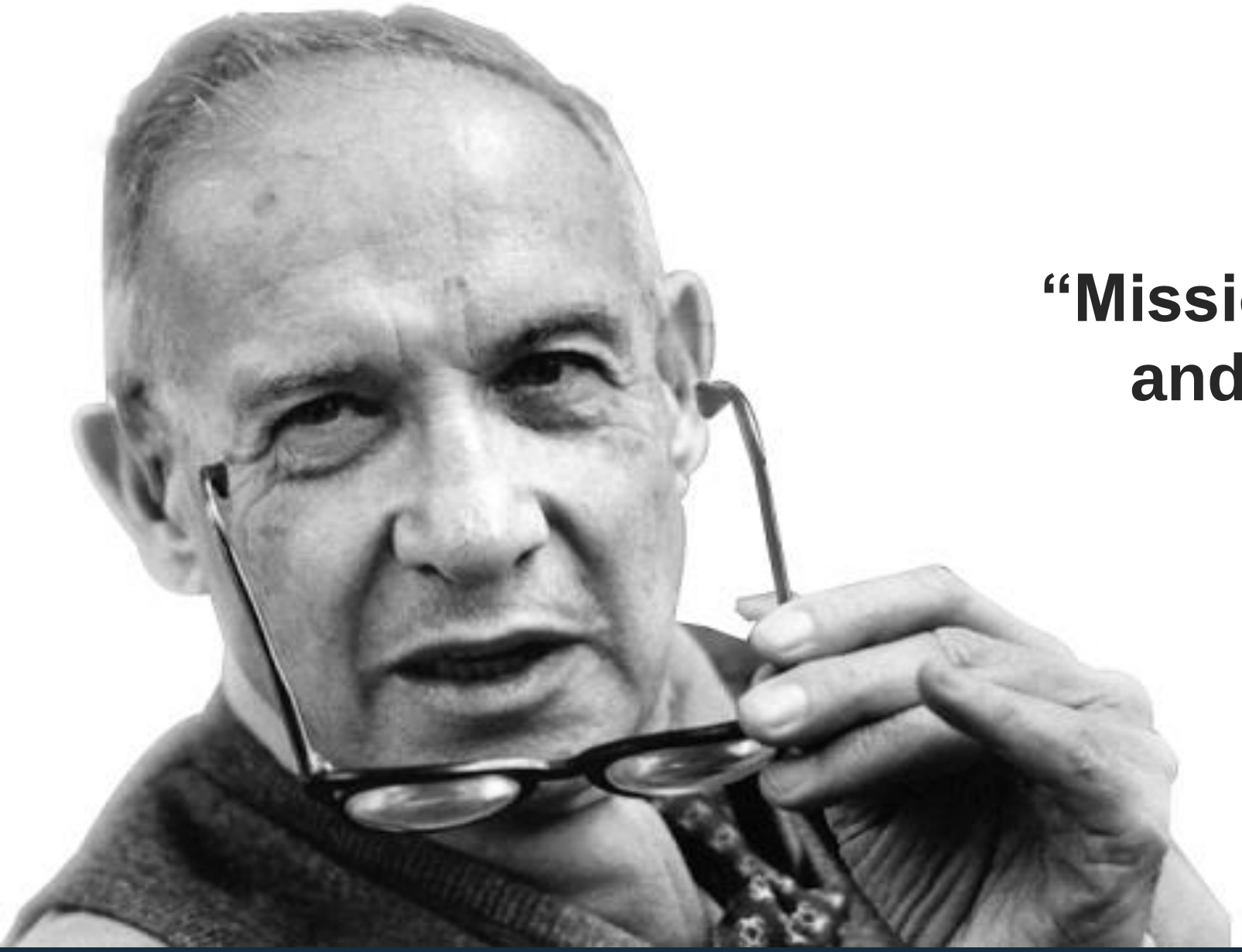
6 Companies, 23 offices, 1300 employees in a blink of an eye

What Was The Problem?

Conventional Strategy, Changing Threat Landscape

- Handful of resources with pockets of knowledge and various layers of security contained within each unique infrastructure.
- Existing security postures were defined by the tools that were in place on each network with the workstation patching being the only practice that was commonplace.
- Maturity of implementation and risk mitigation varied based on resource availability, their security background and the tools that were in place on each network.
- The pressure to achieve a proactive stance regarding these corporate risks within an increasingly challenging business environment, constantly shifting threat landscape and amplified regulatory compliance was immense.

To meet these demands, we needed to evolve…



“Mission defines strategy, and strategy defines structure.”

- Peter Drucker-

Enterprise Security Workforce Mission

- Create the culture, frameworks and processes required to address cybersecurity, enhance decision making and better protect Polaris and our customers.
- Focus on attack prevention, exposure avoidance, breach detection and incident response through continuous monitoring and data analytics.
- Understand the external threat landscape to determine appropriate action ensuring the effectiveness of implemented security controls while harnessing actionable intelligence and insights for a deeper look into the corporate threat landscape.
- Ensure continual improvement to face tomorrow’s security challenges while staying aligned with the security priorities that support Business Unit needs and Corporate strategies.

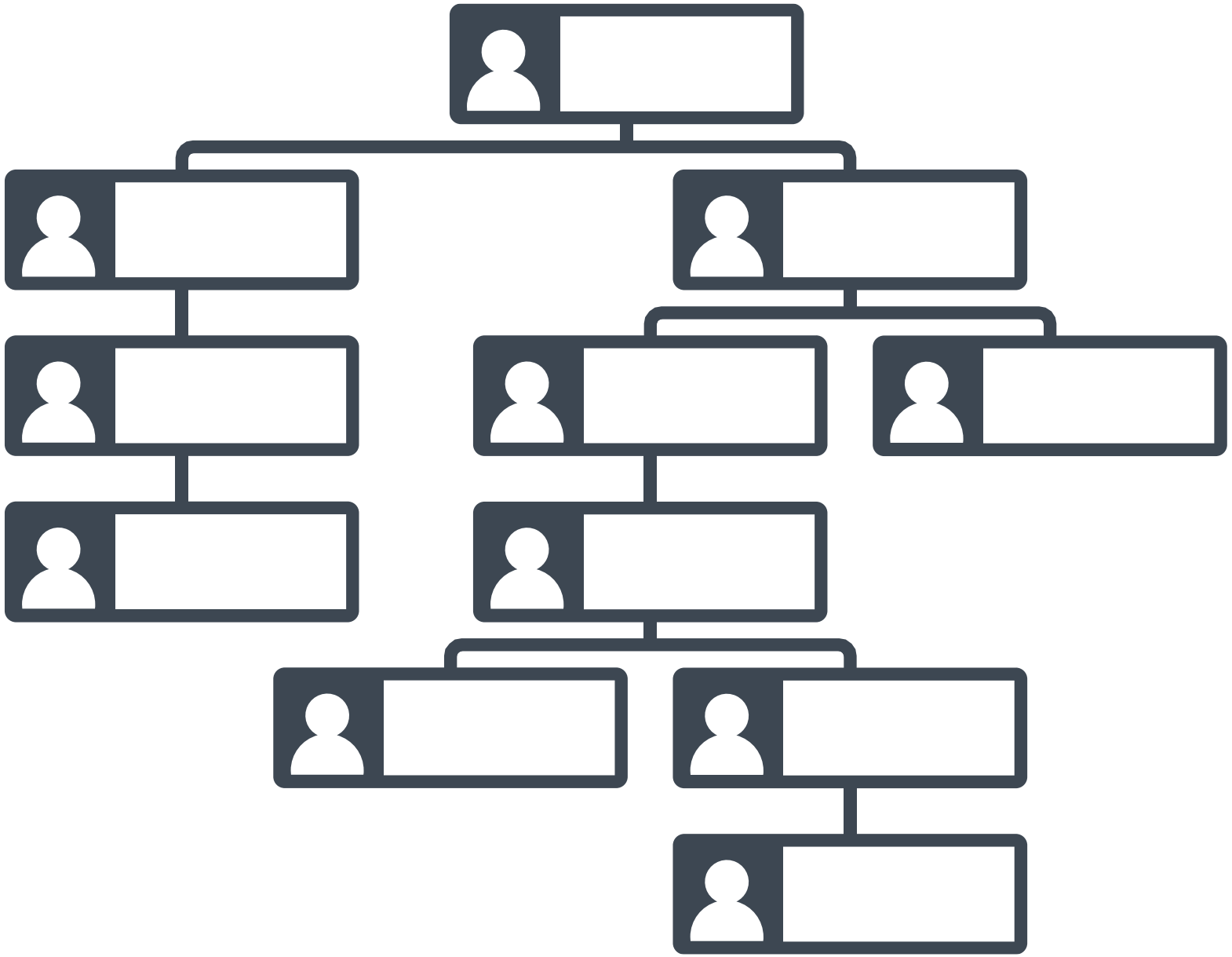
Enterprise Security Workforce Strategy

- Our strategy required us to break free from a model where the expertise was blended across all team members.
  - **Network Defenders** cannot also be **Security Engineers**, focusing, at times, too much on the care and feeding of security tools and new engineering efforts rather then protecting the network.
  - **Network Defenders** cannot also be **Product Owners** focusing, at times, on specific tools creating silos that were not conducive to collaboration and transparency.
  - **Network Defenders** cannot also be **System Administrators**, focusing, at times, too much on IT and compliance tasks.
- Conventional strategies works fine in small teams, but does not scale as we worked to integrate the six Polaris companies, grow the security team, add endpoints to the network, and expanded our toolsets.

Enterprise Security Workforce Structure

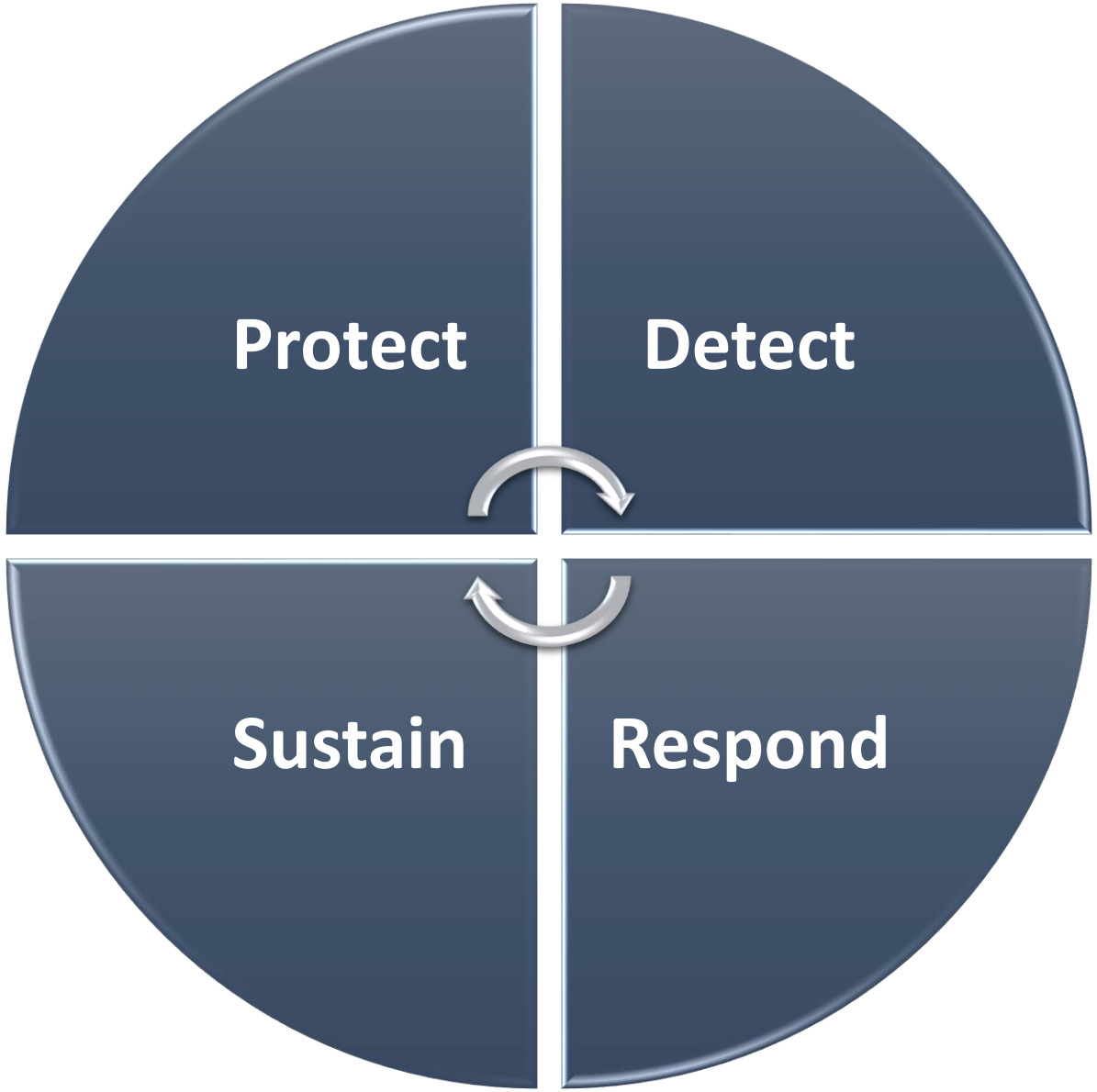
- We needed to consider operating with a more defined workforce structure that ensured we were covering down on all applicable areas of security.
- The goal was to align our workforce based on capability areas, rather than specific tools.
- Given our customer base, we decided to leverage DoD/DISA standards and included the Chairman of the Joint Chief of Staff Manual (CJCSM) 6510.01b
    - Defined a way to maintain a proactive, progressive, and coordinated approach to detecting and responding to security events and incidents that can adversely affect the network
    - Outlined an integrated capability to allowed for a consistent, repeatable, quality driven, and measurable approach that was easily leveraged
    - Provided the requirements and methodology for establishing, operating, and maintaining a robust security incident handling capability for routine response to events and incidents

What Did This Mean?



This was NOT an Org Chart

This was a way to ORGANIZE



Who Uses This Model?

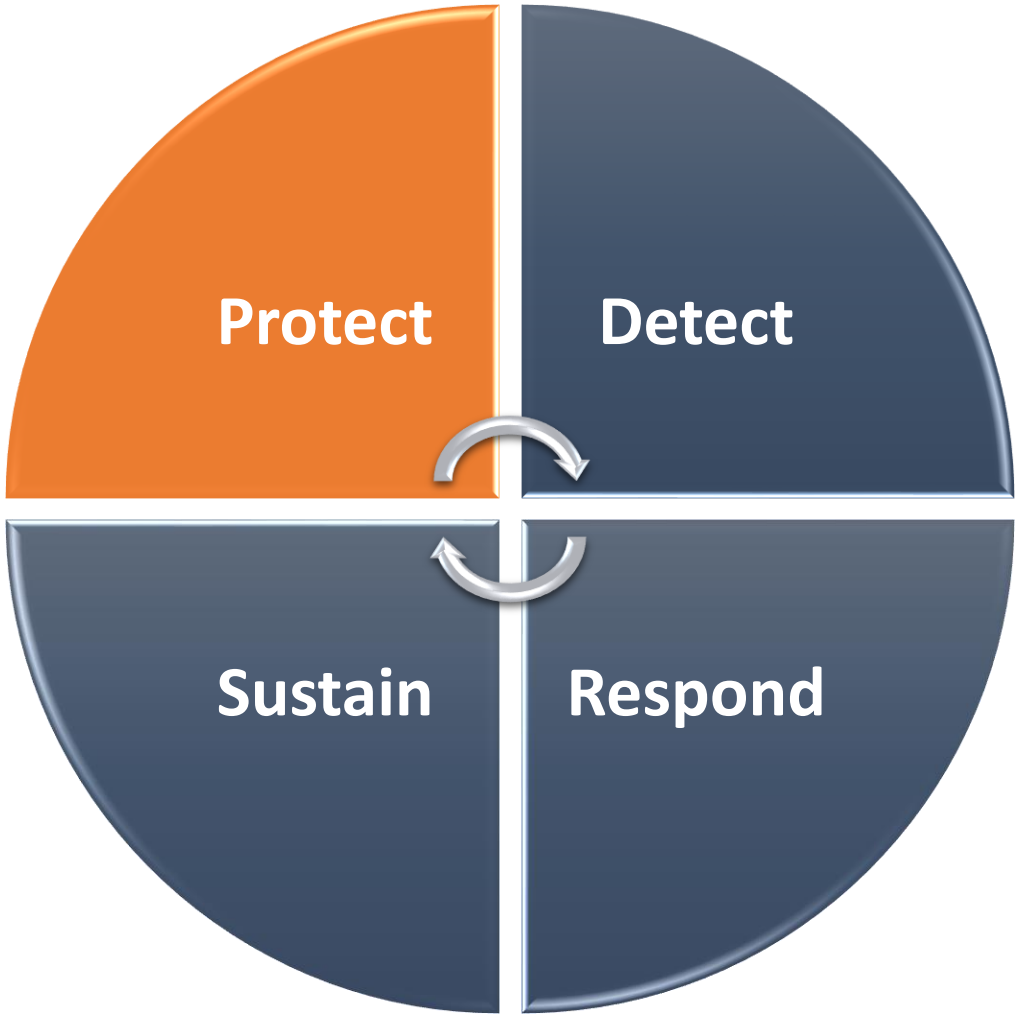
Information Security Workforce Usage

DoD Cyber Security Service Providers (CSSPs)	**Protect, Detect, Respond, Sustain**
Defense Information Systems Agency	**Protect, Detect, Respond, Sustain**
Missile Defense Agency CERT	**Protect, Detect, Respond, Sustain**
NSA Infosec Evaluation Methodology (IEM)	**Protect, Detect, Respond, Sustain**
Carnegie Mellon Software Engineering Institute (SEI)	**Protect, Detect, Respond, Sustain**
US-CERT	Prepare, **Protect, Detect, Respond**
Nation Institute of Standards and Technology	Identify, **Protect, Detect, Respond**, Recover
Microsoft	**Protect, Detect, Respond**

And many, many more…..

How Did This Work?

Enterprise Security Workforce Structure



- Everything we do to harden the network so that when the adversary arrives, the doors are closed

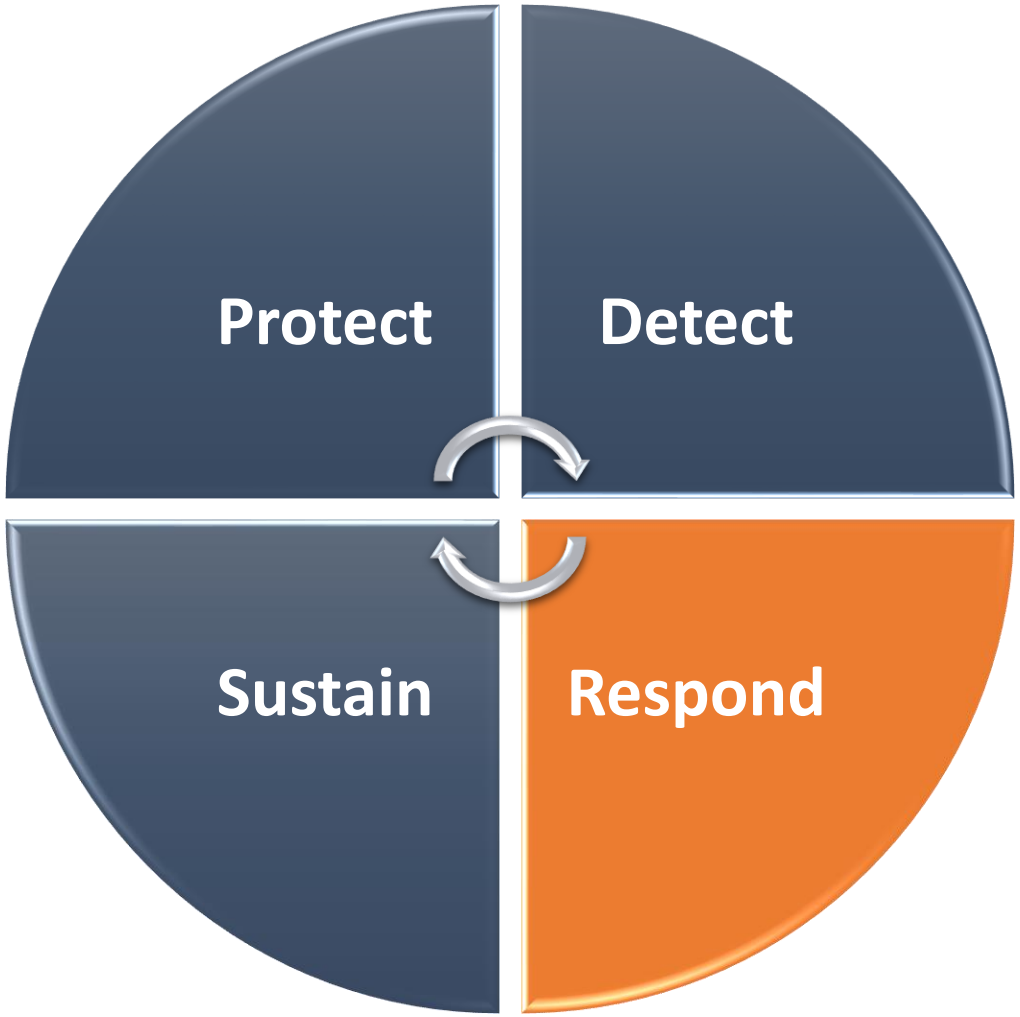
- Proactive measures that taken to defend networks, systems and data
  - Routine (scheduled) and targeted vulnerability scanning and reporting
  - Patch Management
  - Endpoint Security
  - Secure Authentication
  - Signature Updates
  - Penetration Testing/Red Team
  - Ports, Protocols, and Services
  - User Education

Enterprise Security Workforce Structure

- In the event that an adversary gets through despite PROTECT measures, we have to know that it happened in order to do something about it.

- Activities geared at finding adversarial activity:
  - Intrusion Detection
  - Continuous monitoring
  - Detect and categorize security events/incidents
  - SIEM tuning, optimization, content creation, report generation
  - IDS tuning/optimization, content creation
  - Log analysis (e.g. web logs, DNS logs)
  - Adversary Tactics, Techniques, and Procedures (TTPs)
  - Hunt activities (hunting for adversary activity when there is no Indicator of Compromise)

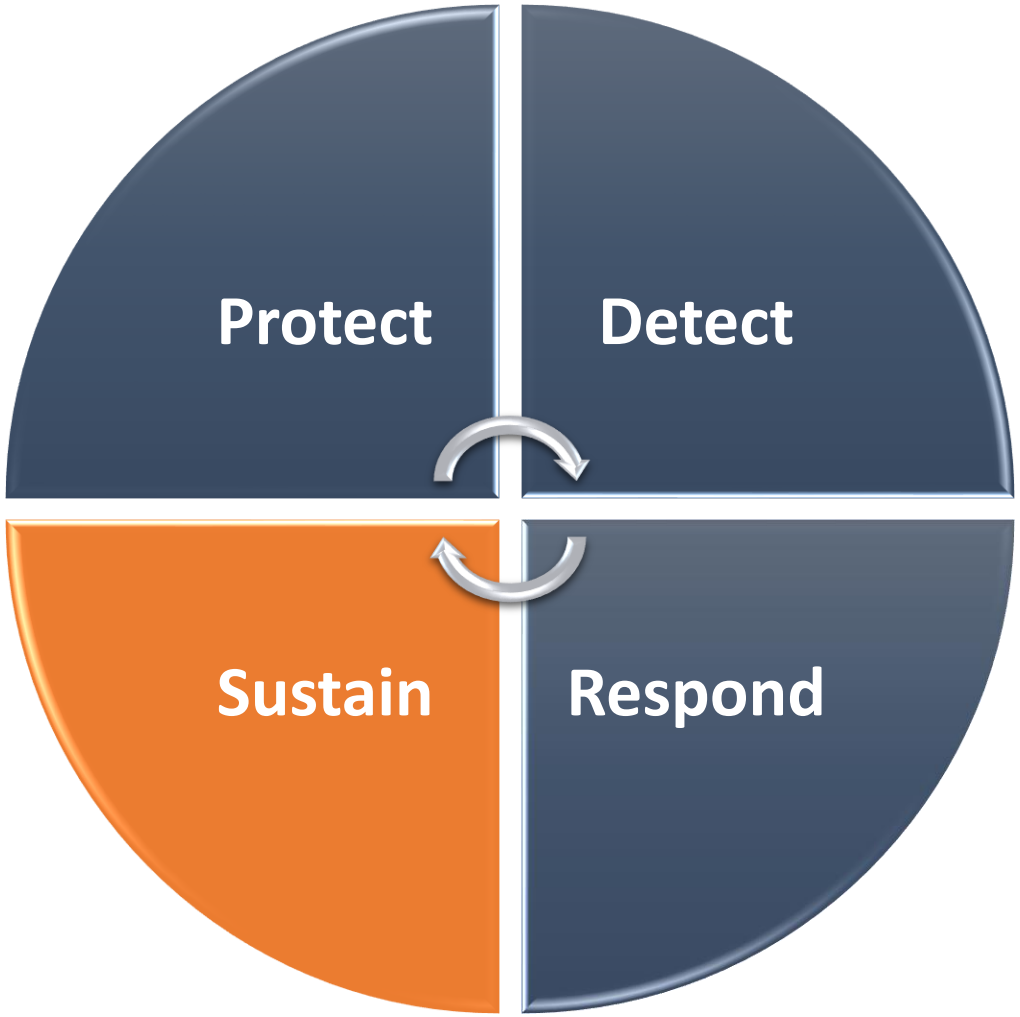
Enterprise Security Workforce Structure



- In the event that an adversary has been discovered by DETECT measures, we need to minimize damage and restore business capabilities as soon as possible

- Coordination and management of the response to rapidly identify the full scope of a breach and eradicate the threat
  - Investigates cases
  - Determines vector and assesses damage
  - Takes action to stop the event if ongoing
  - Removes malicious code from the network
  - Restores capability
  - Creates detailed technical reports for leadership
  - Makes recommendations to prevent future incidents
  - Develops/maintains Incident Response Plan

Enterprise Security Workforce Structure



- Application of expert strategies and evaluation of emerging technologies to ensure the PROTECT, DETECT and RESPOND teams can do their jobs effectively

- Operations (Management)
  - Training Management (vendor, professional certifications)
  - Policy creation & compliance adherence
  - Report writing for senior leadership
  - Documentation tracking and maintenance
  - Communication with other external organizations
  - Dissemination of orders, threat intel, other security information
  - Weekly Cyber Threat Update briefing
- Systems and Technology (Engineering)
  - Care and feeding of security systems/tools
  - Evaluation of emerging technologies
  - Vendor relationships and licensing
  - Security architecture and engineering efforts

What Was Our Approach?

Enterprise Security Workforce Approach

This strategic initiative created a security community where people thrive, performance excels and risk is reduced.

NOW

Build The Foundation

Assemble a state-of-the-art security team while optimizing the use of available resources

NEAR

Realize The Effectiveness

Accelerate an approach that provides a holistic network defense strategy delivered via a set of highly specialized services

FUTURE

Advance The Mission

Achieve a financial, operational, and strategic structure enabling scale and growth

NOW: Build The Foundation

- Transform into a **world class Security Operations Center (SOC)** focused on attack prevention, breach detection and incident response through continuous monitoring and data analytics.
- Align **workforce structure** based on capability areas, rather than specific tools and separate the duties of network defenders from security engineers promoting cross-training and deterring single points of failure.
- Apply **agile** and expert strategies to evaluate emerging technologies ensuring **continual improvement** in order to face tomorrow's security challenges while staying aligned with the security priorities that support Business Unit needs and Corporate strategies.
- Create a **Security Innovation Program** encouraging the development state-of-the-art solutions from industry awareness and insights collected during the active defense of the network.
- Instill a customer service approach focused on demonstrating the value of the team as a **trusted partner** and **thought leader** to the business.
- Establish **strategic partnerships** and relationships with vendors that enhances the overall security posture while reducing costs.

NEAR: Realize The Effectiveness

- Define & Document Battle-Rhythms
  - Determine lines of demarcation
  - Break down tools and processes to areas of responsibilities
  - Identify gaps in knowledge or training
  - Define clear roles and responsibilities
- Staggered Shift for Success
  - Adjust schedules to WFO as we shift into new structure
  - PROTECT goes first followed by DETECT & RESPOND shortly thereafter
  - SUSTAIN runs in parallel
- Transition, Train, Tune & Trust
  - Transition non-network defense activity
  - Train our teams for techniques used in each toolset
  - Tune procedures to ensure process and documentation are clear
  - Trust (but verify) our teams are learning & growing

FUTURE: Advance The Mission

- Invest in Functional Leads
  - Promote to drive consistency across teams
  - Integrate battle-rhythms into singular unified platform
  - Educate customers to how we operate and are engaged moving forward
- Instantiate Multi-SOC Model
  - Deploy centralized SIEM and produce a single view into each network
  - Share data, find synergies and merge workflows
  - Cross training and shared workload of individual networks
  - Consolidate Incident Response Database into Salesforce
  - Create repeatable process for future SOCs
- Integrate Teams
  - Realize scalability and cover down for each other (2nd set of eyes, holidays, etc)
  - Deeper On-Call Schedule and Availability
  - Security Continuity ensuring eyes are always on scope as we strive for 24X7 coverag

What Were The Benefits?

Enterprise Security Workforce Benefits

- Advising the business on managing the risk to information assets, including those related to security, privacy and regulatory compliance
- Collaborative team of security professionals proficient in Cyber Risk Intelligence, Security Data Analytics, Internal Control & Assurance and Risk Consultancy
- Effective approach that aligns the capacity and skills of all internal security professionals to deliver a premier service
- Structured set of services that provide impartial, third party oversight for today's stringent security standards

Built an effective, forward-leaning security and corporate risk program

POLARIS
ALPHA

Eric Schlesinger

Chief Information Security Officer

✉: eric.schlesinger@polarisalpha.com

☎: 443.539.3405

☎: 443.871.5268

💻: www.polarisalpha.com