



accenture

High performance. Delivered.

Moving Beyond Boundaries

Cyber Security and Data Protection

Bud Horton

August 5, 2009

The numbers tell the story

10,000

The number of times the Air Force is attacked each day in cyber space.

80 percent

The percentage of spam e-mails received by the Air Force.

One trillion bytes

The extent of data illegally extracted from Air Force networks.

SOURCE: Air Force Cyber Command Web site, 4/08, <http://www.afcyber.af.mil/news/story.asp?id=123094076>

The reality of a new era of warfare

"In an Air Force that is a lot of times focused on kinetic activity—read that read as F-16 (Fighting Falcons) and 2,000-pound bombs—not at warfare conducted in a different manner at the speed of light, cyber operations require some new thinking."

"Our trouble today is that we're always shooting behind the rabbit. We wait for the latest exploit, and then when something bad happens, we figure out how to fix it."

Maj. Gen. William Lord
Commander of Air Force Cyber Command (Provisional)
May 2009

SOURCE: Air Force Cyber Command Web site, 5/08, <http://www.afcyber.af.mil/news/story.asp?id=123149009>

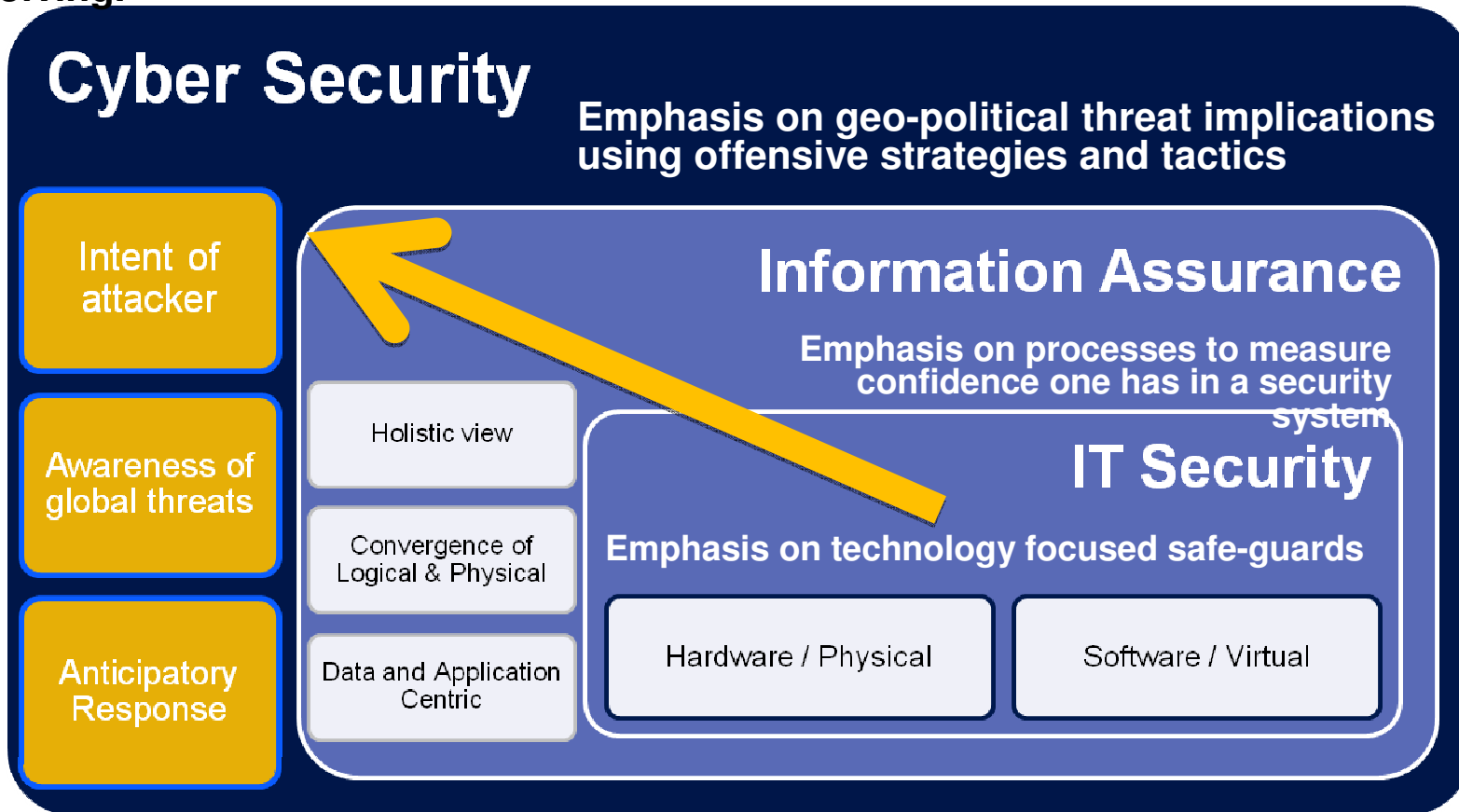
Objectives

This presentation focuses on:

- **The landscape.** New realities of today's cyber security environment and the imperative for offensive strategies.
- **The imperative.** Predictive intelligence, data protection and information sharing among stakeholders.
- **The stakeholders.** New roles for key stakeholders—from defense and government to the private sector.
- **The solution.** Innovative solutions for cross-stakeholder incident sharing without compromising security.
- **The future.** A new model for situational awareness
- **The results.** Situational metrics development between government and the private sector.

Evolution of Information Security

“The uniqueness of cyberspace can best be described by three attributes: volume, speed, and convergence. More than the speed of the communications, the rate of change of cyberspace, and the applications that use it, is continuous, making this domain ever evolving.” *

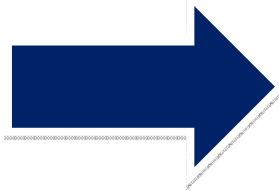


* Lieutenant General Keith Alexander Commander Joint Functional Component Command for Network Warfare

The role of information sharing

All stakeholders centered around a data-centric, multi-level security architecture:

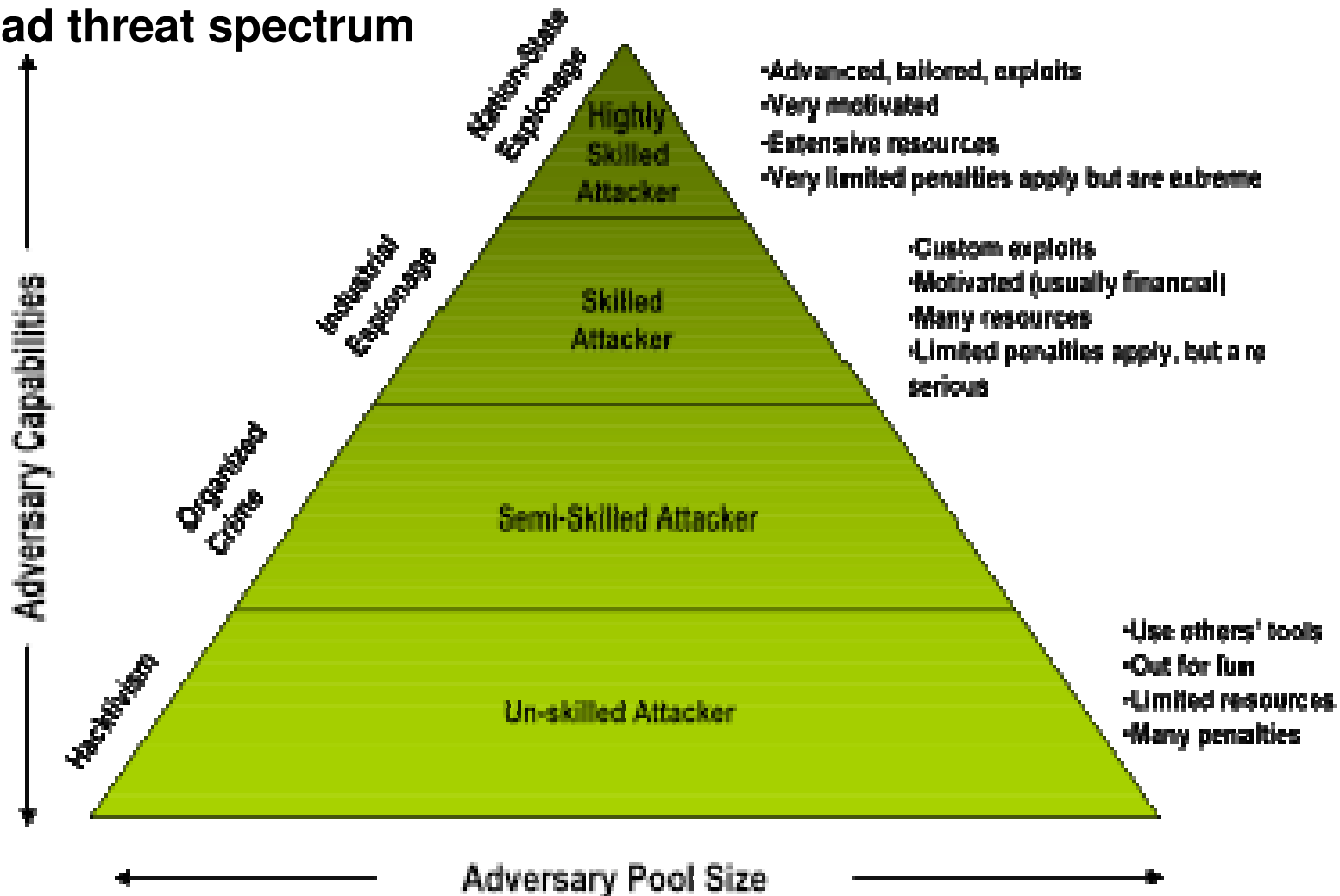
- Command and control
- Warfighters
- Intelligence community
- Law enforcement community
- Allied nations
- Government agencies
- Industry



- Ability to collaborate across different security levels
 - Unclassified
 - Confidential
 - Secret
 - Top Secret
- Ability to apply collaboration across discrete sensitivities
 - Unclas Rel FBI
 - Unclas Rel ICE
 - Unclas Rel NYPD
- Ability to apply collaboration within a security level
 - Secret Rel X
 - Secret Rel Y
 - Secret Rel Z

Facing a complex threat spectrum

Broad threat spectrum



Working against tough challenges

Complex challenges

- New demand
- Opportunity
- Public access
- Device unawareness
- Limited resources
- Time-intensive solution

Meeting policy expectations

The Comprehensive National Cybersecurity Initiative

- Establish front lines for cyber defense
- Define the critical defensive tools and techniques for effectiveness
- Shape the future environment
- Begin work on foundational initiatives

The imperative for offensive strategies

Ideal: “smoke ‘em out”

Look for traces of threats on public networks

Analyze suspicious activity before it shows up in historical logs

Spot live and active malware that can compromise identifies

Today: “block and tackle”

T=24 hours

Block virus signatures and network intrusions

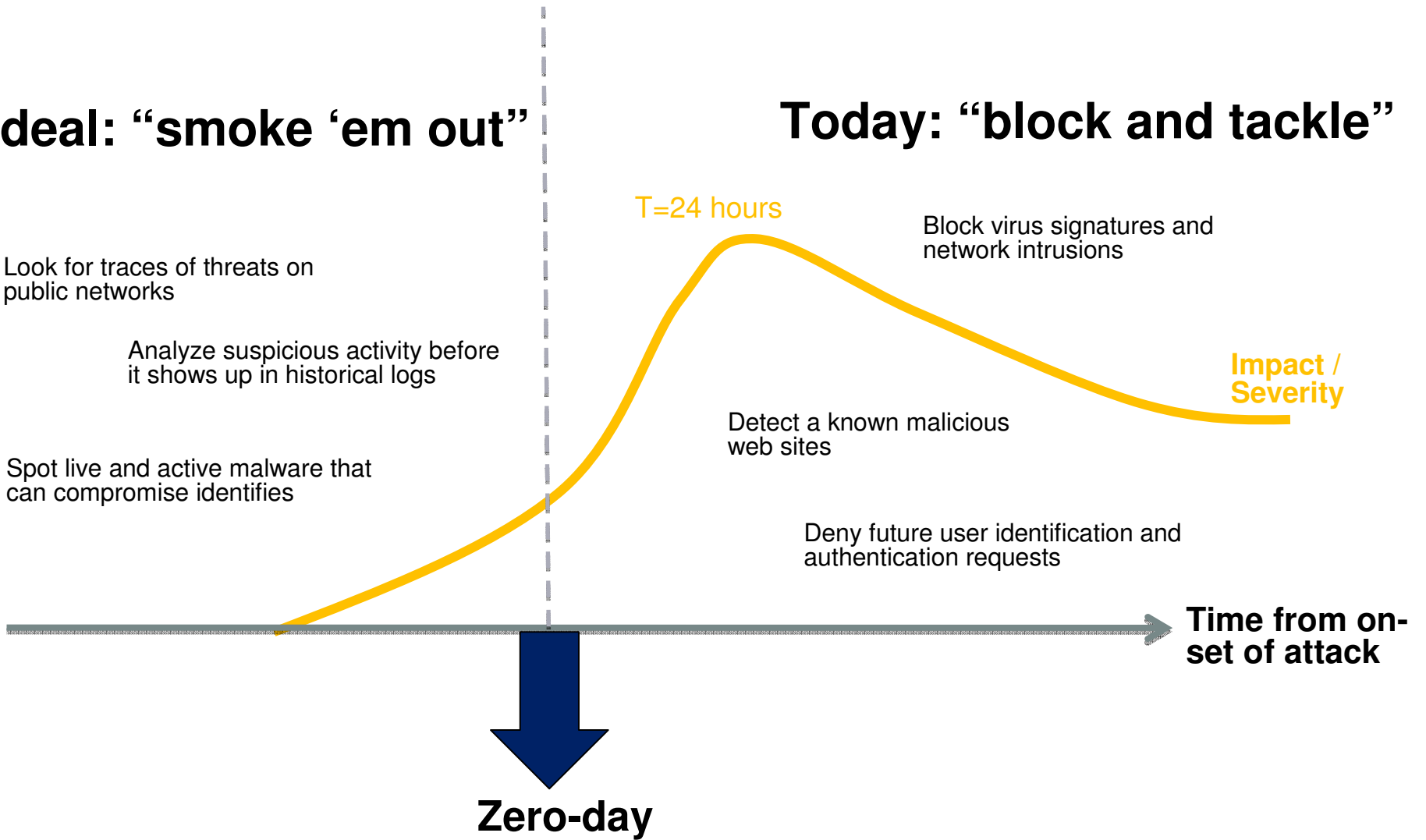
Detect a known malicious web sites

Deny future user identification and authentication requests

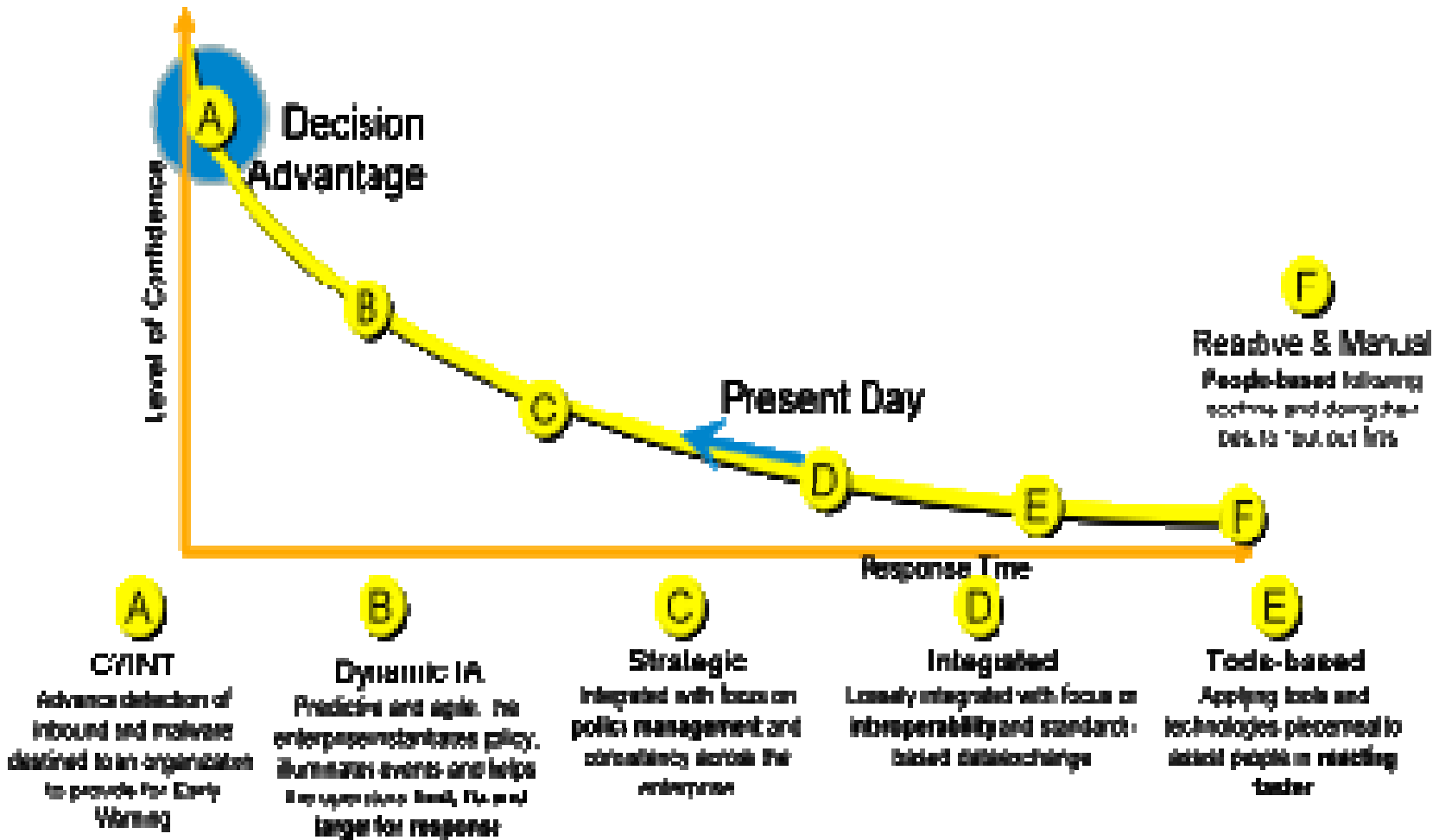
Impact / Severity

Time from on-set of attack

Zero-day



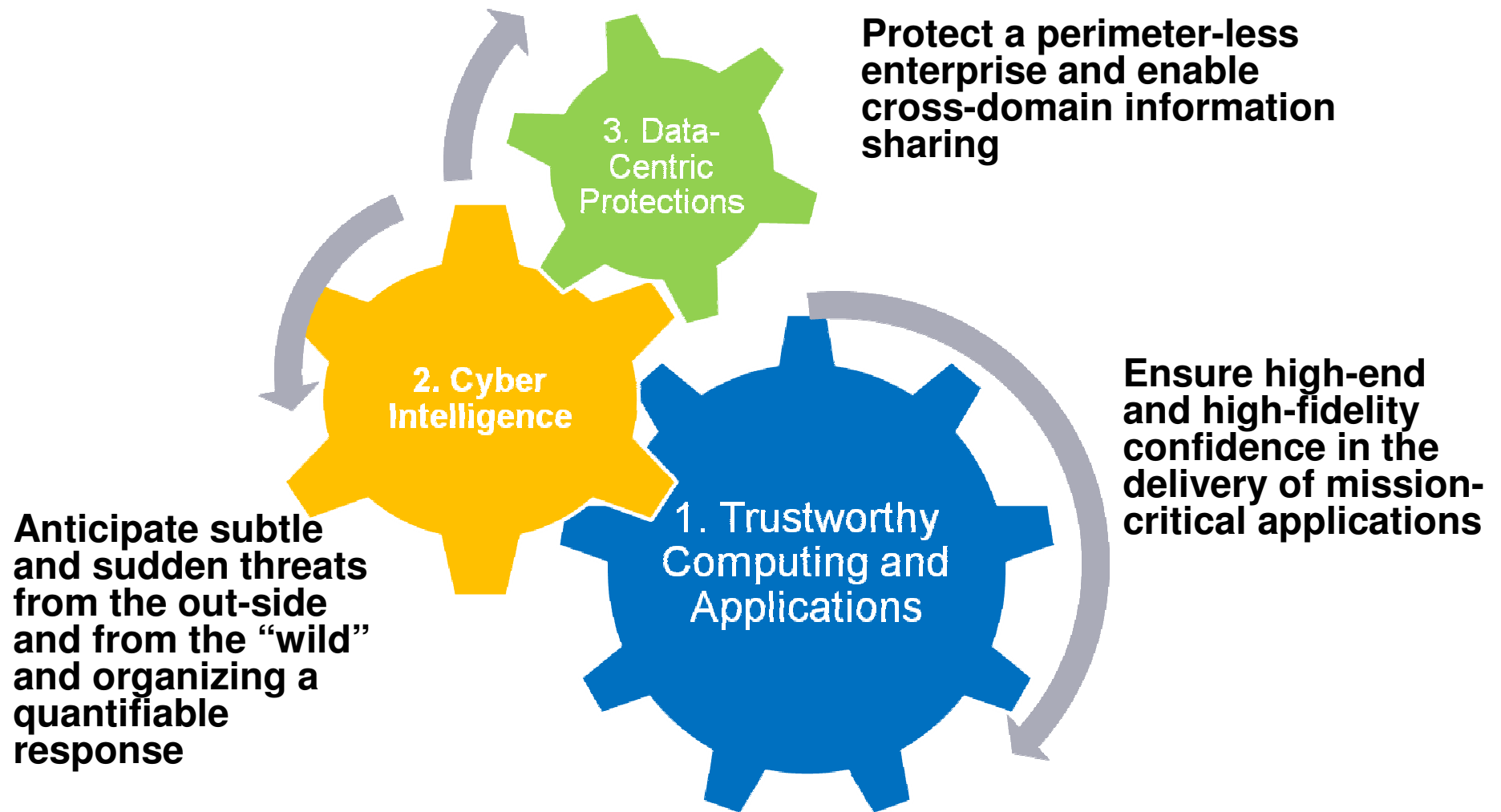
The spectrum of cyber security maturity



The secured enterprise- An effective offense is a holistic one

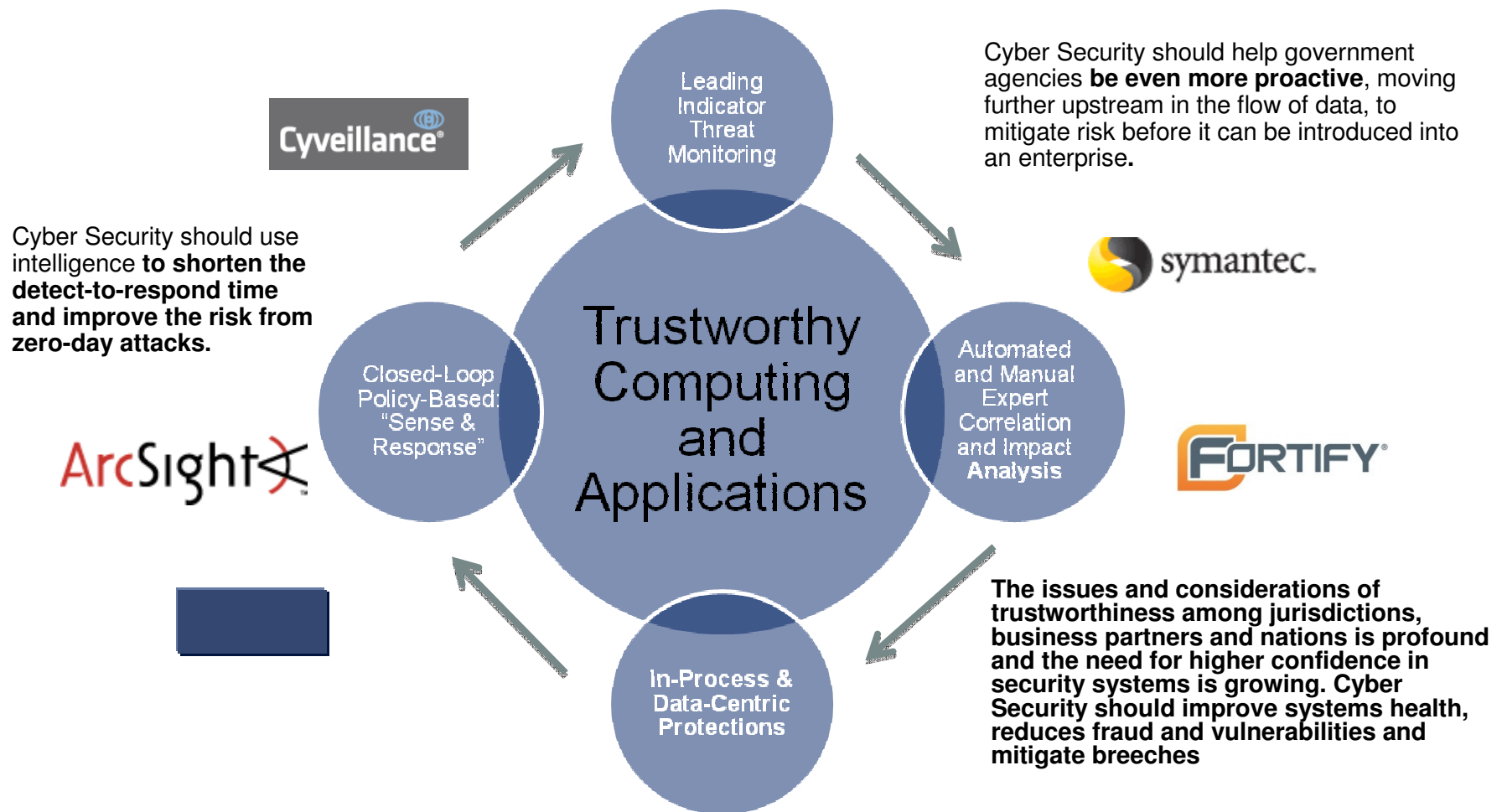


A multi-faceted cyber security strategy



Sustain the design, implementation and operation of trustworthy applications and compute environments

Cyber Security capabilities marry expert cyber security skills and leap-ahead technologies to anticipate emerging threats and effectively manage continuously evolving global-scale risks.



A trusted system- All protection mechanisms work together

- Proper security concepts, controls, and mechanisms are **integrated before, and during the design and architecture**
- Security is engineered, implemented, tested, audited, evaluated, certified and finally accredited

Some of the methods to evaluate how well a system meets their security requirements:

Trusted Computing Base and Security Perimeter

- Combination of hardware, software and controls to enforce policy
- Subset of the complete information system
- Trusted paths must be established across physical and virtual perimeters without exposing the TCB to security vulnerabilities

Policies, standards, baselines, guidelines and procedures

- Top tier documents that define the scope of the security needed
- Define compulsory requirements and are tactical in nature (criteria set forth by NIST, DoD Trusted Computer System Evaluation)
- Step-by-step actions of implemented controls

Common Criteria

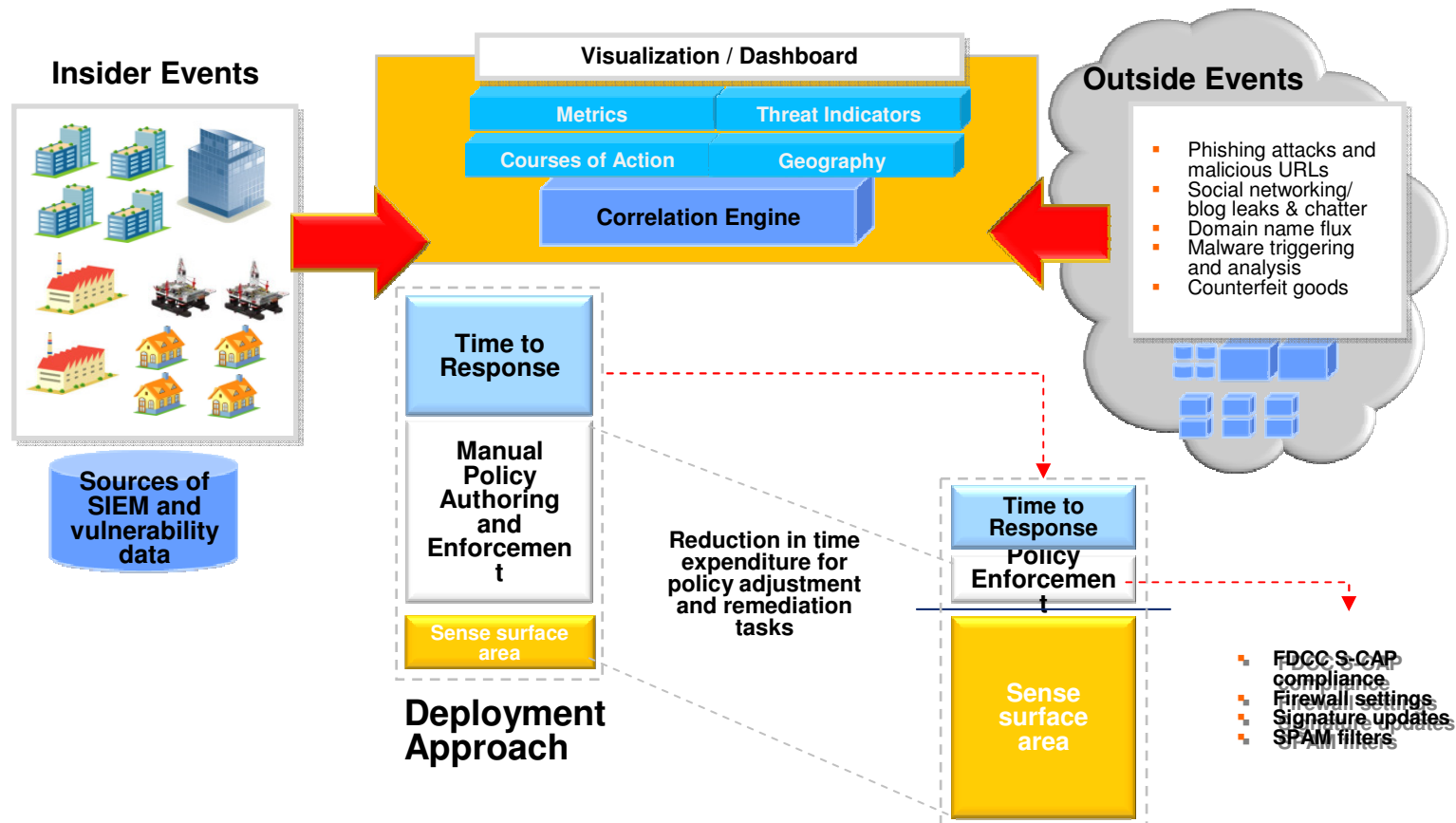
- Various levels of testing and confirmation of a systems capabilities
- Buyer confidence in the security of evaluated products

Certification & Accreditation

- Certification is a comprehensive evaluation of features
- Determine whether system network or major application satisfies the desired security goals - given the environment and configuration

Cyber situational awareness notional description

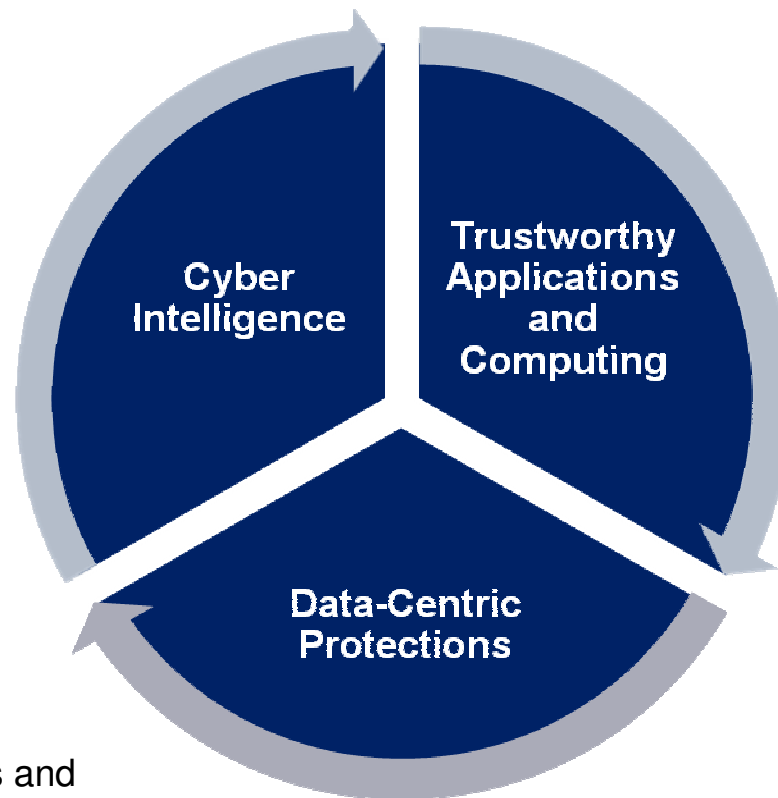
Cyber intelligence coupled with “Dynamic” Cyber Defense turns insight of your operational stance into organized action that reduces the time to respond and increases mission resiliency



Accenture Threat Analysis Center (ATAC) of Excellence

ATAC helps federal, state & local agencies and critical infrastructure organizations advance their regulatory compliance by making informed decisions and taking timely action on cyber threats. The center features concentrated skills, core staff and innovative capabilities across 3 areas:

- Decision support and insight onto emerging threats
- Information fusion of mal-ware activity and cyber forensics to generate meaningful actions
- Integrated monitor, sense and response



- Hardened custom off the shelf applications
- Software scans and **expert** code reviews
- Cloud and virtualization security
- FDCC readiness and compliance

Other ...

- Data Residency
- Language
- US Citizens
- Clearances
- Agency procedures & Policies
- Physical environment
- FISMA , NIST and agency-specific STIG requirements

- Secure Hosting
- IP v6 readiness and enablement
- Secure DNS solutions
- **Data privacy and encryption**

Questions?

Contact Information

Bud Horton

Accenture

Executive Director

Accenture Technology Consulting—Security

henry.h.horton@accenture.com

+1 703 947-1262



A multi-faceted cyber security strategy

Dynamic information assurance

Enhancing traditional security by combining analytics, decision making tools and predictive security mechanisms

Situational awareness

Seeking out the indications of malware and attacks and organizing a quantifiable response

Threat management

Architecting and engineering applications and systems to be resilient in the face of known and unknown threats