



TECH BELT

Technology Summit



Your Most Strategic Business Asset is The Network

Strategic CIOs leverage the network to fuel business growth

Scalable adaptive and resilient architecture

Balance of performance, intelligence and simplicity



TECH BELT
Technology Summit

Information Security

An Understanding and Overview



Bio

- Security Systems Sr. Advisor for Dell SecureWorks
- Over 15 years experience in security operations, threat intelligence, and incident response
- Provides SOC Thought Leadership and Consulting to Fortune 500 customers



TECH BELT

Technology Summit

Outline

- Why is Information Security Important
- Key Areas of Information Security
- Types of Threats
- Current Threat Landscape
- Tying It All Together
- Questions and Answers



TECH BELT

Technology Summit



U.S. DEPARTMENT OF
ENERGY





Why is Information Security Important?

January 1, 2014 – April 29, 2014 there have been 260 disclosed breaches resulting in 8,329,265 records exposed*





Why is Information Security Important?

- Protection of sensitive information
- Protection of brand reputation
- Protection of networked systems (botnets, etc.)





Key Areas of Information Security

- Access controls
 - Passwords and password complexity
 - ACL (Access Control Lists)
 - Administrative privileges
 - Physical Security





Key Areas of Information Security

- Network Security
 - Egress filtering
 - Vulnerability management
 - Patching
 - Anti virus/HIPS (Host Intrusion Prevention Systems)
 - Application white listing
 - IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems)
 - Penetration Testing





Key Areas of Information Security

- Governance Risk, and Compliance
 - Governing bodies
 - Compensating controls
 - Information security policies and procedures
 - Risk assessments and risk classifications
 - Third party risk assessments
 - Internal/external audit
 - Regulatory obligations





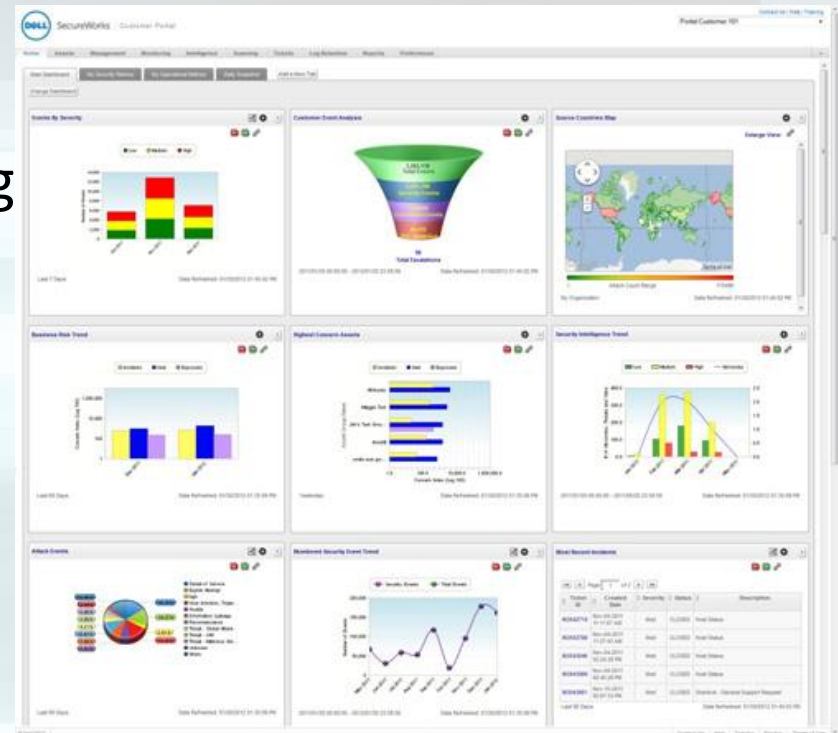
Key Areas of Information Security

- Application and Systems Development
 - Application security assessments
 - Secure coding practice
 - Third party application reviews



Key Areas of Information Security

- Security Operations
 - Security event monitoring
 - Incident response
 - Threat assessments
 - Threat intelligence
 - Daily threat report





Key Areas of Information Security

- Security Awareness
 - Security awareness newsletter
 - Phishing warnings, what to look for
 - Information Security contact for employees
 - Training programs





Current Threat Landscape

– Industry reports:

- Malware advancement
- Mobile attacks
- Mobile malware
- Botnets
- Social Engineering





Current Threat Landscape

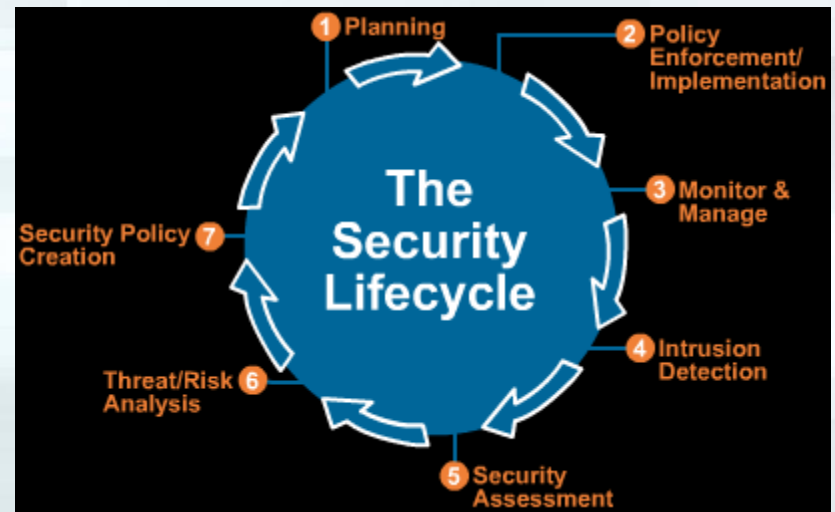
- Other attacks:
 - State sponsored cyber warfare
 - Geo-political cyber attacks
 - Industry specific attacks
 - Brand reputational attacks
 - DDoS





Tying it all together

- Information Security model
- Reduction in attack surface
- Defense in depth
- Incorporating threat landscape into vulnerability management
- Matching penetration testing results into the monitoring program





TECH BELT

Technology Summit

Questions?



TECH BELT

Technology Summit



Your Most Strategic Business Asset is The Network

Strategic CIOs leverage the network to fuel business growth

Scalable adaptive and resilient architecture

Balance of performance, intelligence and simplicity