Application Security Kung-Fu

Competitive Advantage from Threat Modeling

Akshay Aggarwal
Practice Manager (North America & LATAM)
Akshaya AT Microsoft Dot com
ACE Team
Microsoft Information Security

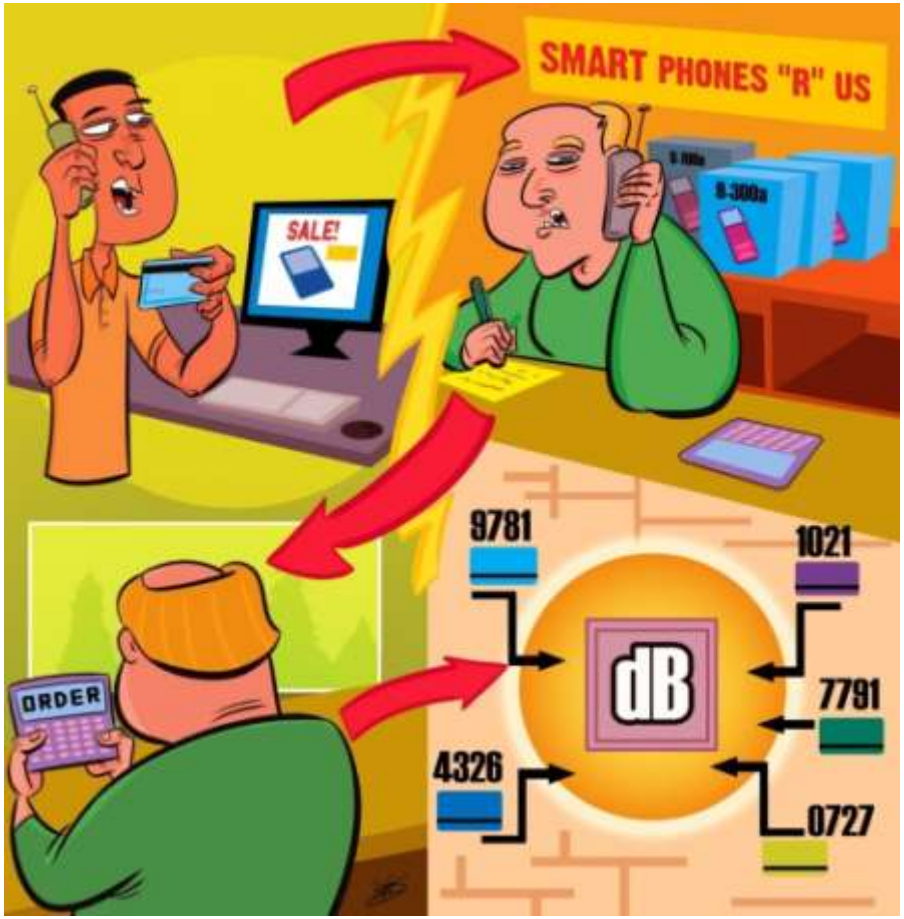
Agenda

- Background
- Information Security (InfoSec) challenges
- Driving security into development
- Threat Modeling
- Bringing it all together
- Conclusion

Trend of Security Breaches

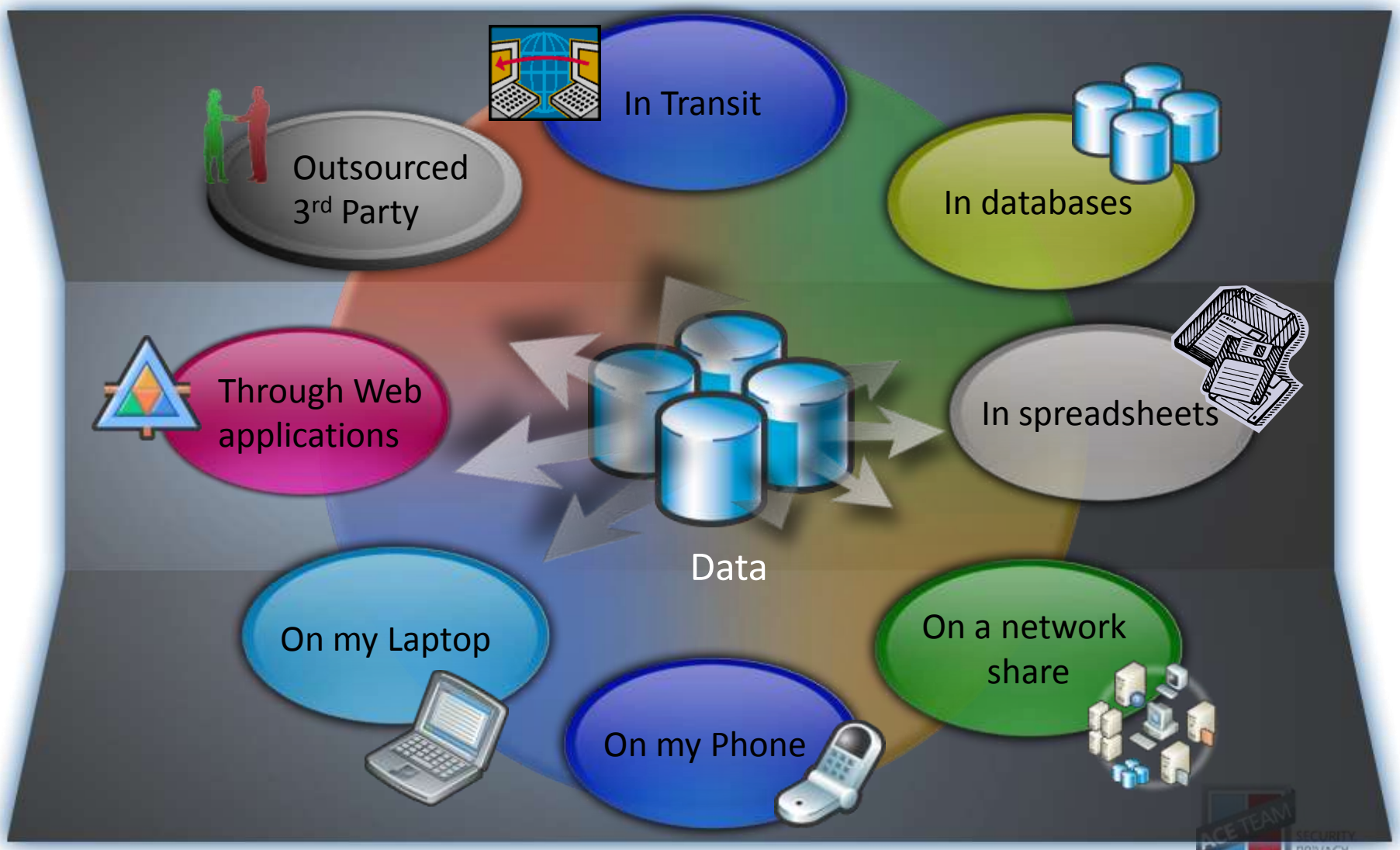
WHAT ASSETS DOES YOUR ORG CARE ABOUT?

Scenario

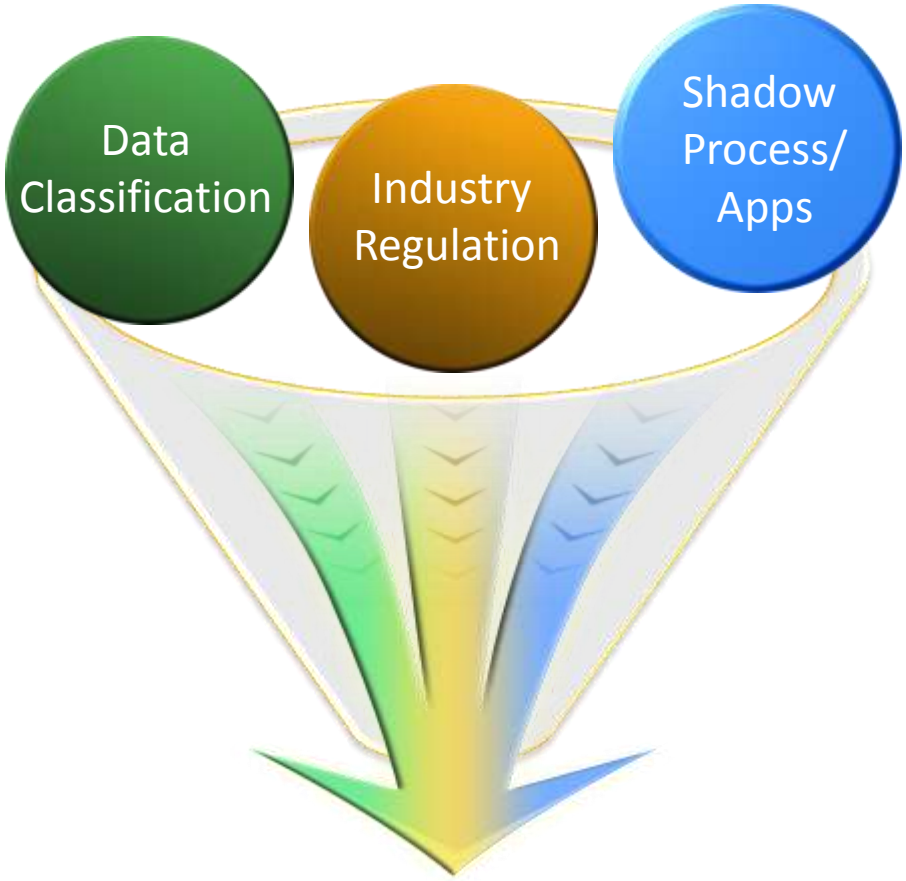


Business as Usual

InfoSec Challenges – Where's the Data

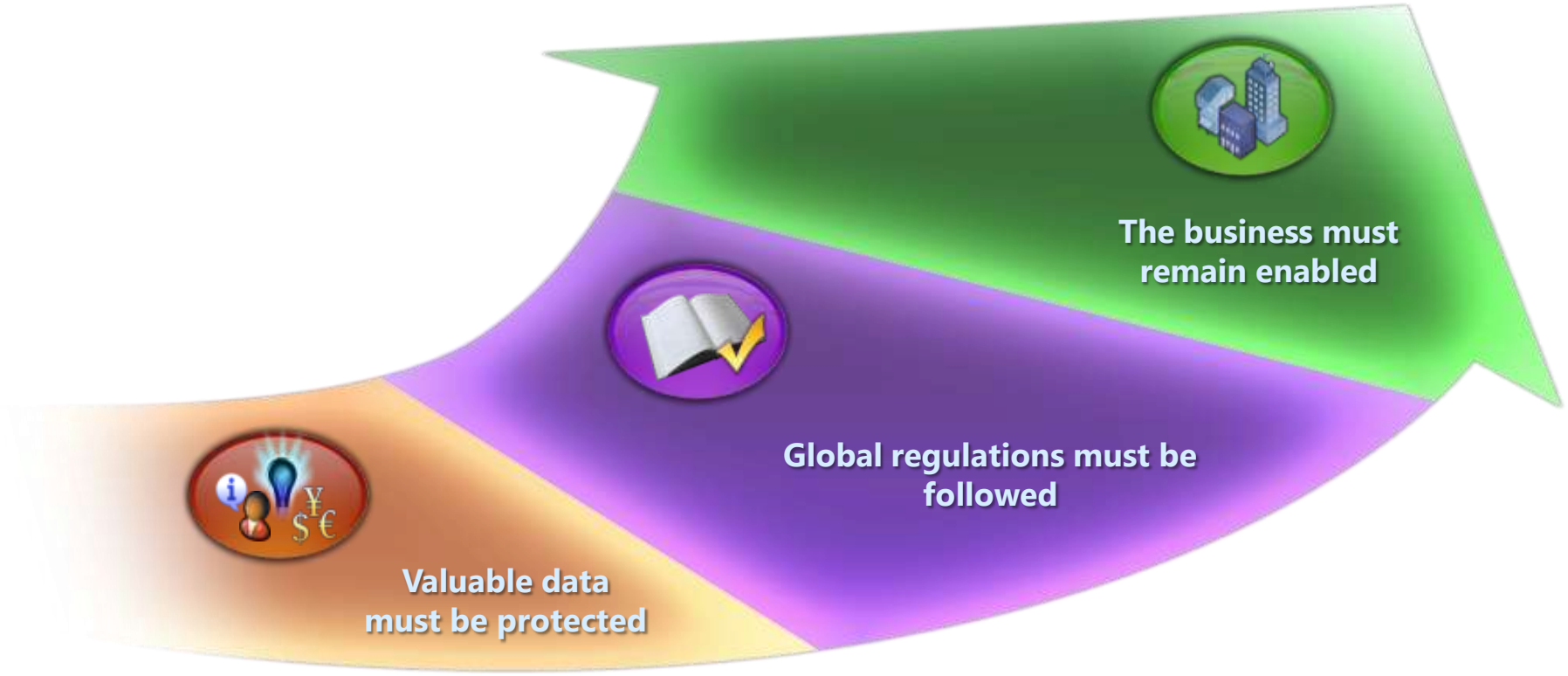


Process Complexities



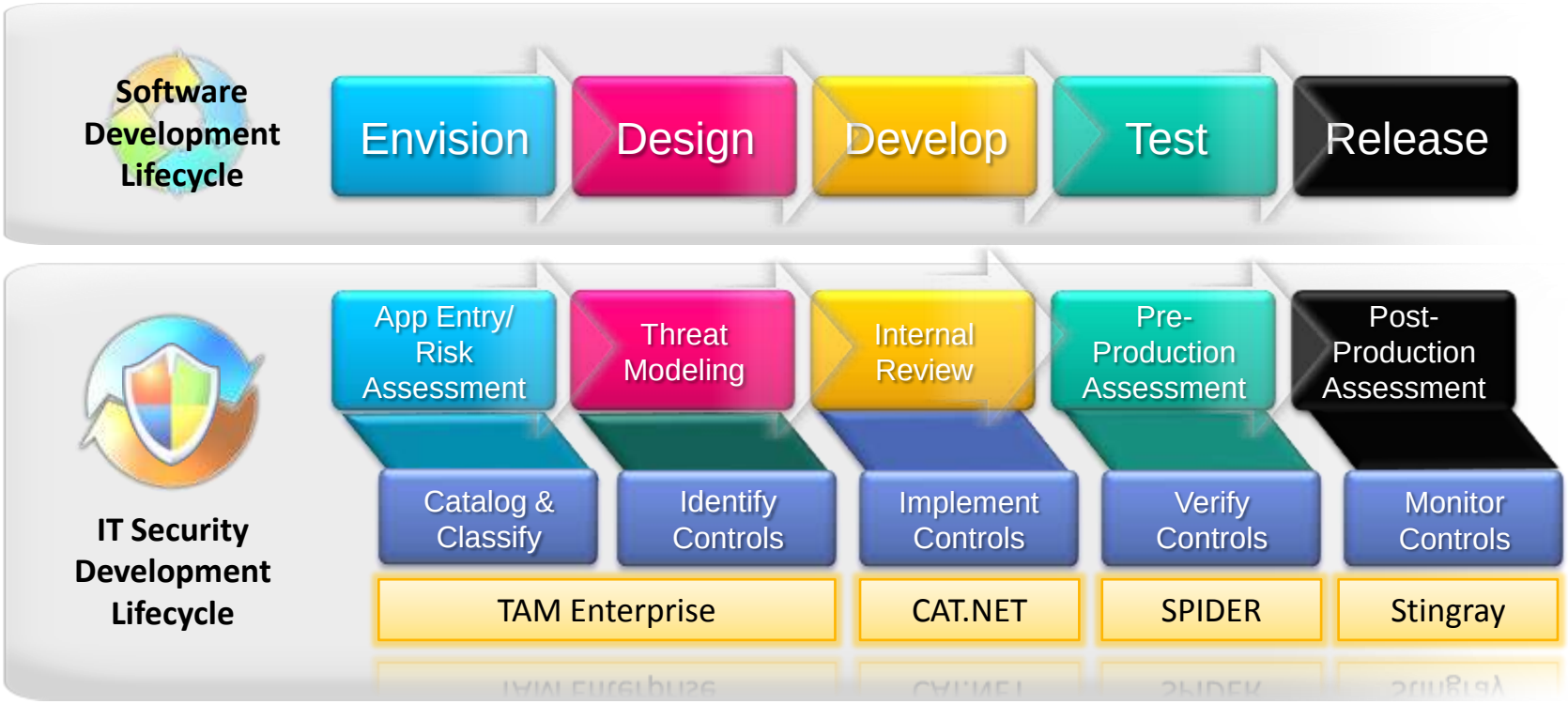
Risk Management

InfoSec Priority



IS THERE A PROCESS DRIVING APPLICATION SECURITY?

Driving Security Into Development



DO YOU ANALYZE YOUR THREATS? HOW?

ACE Security

PROCESS

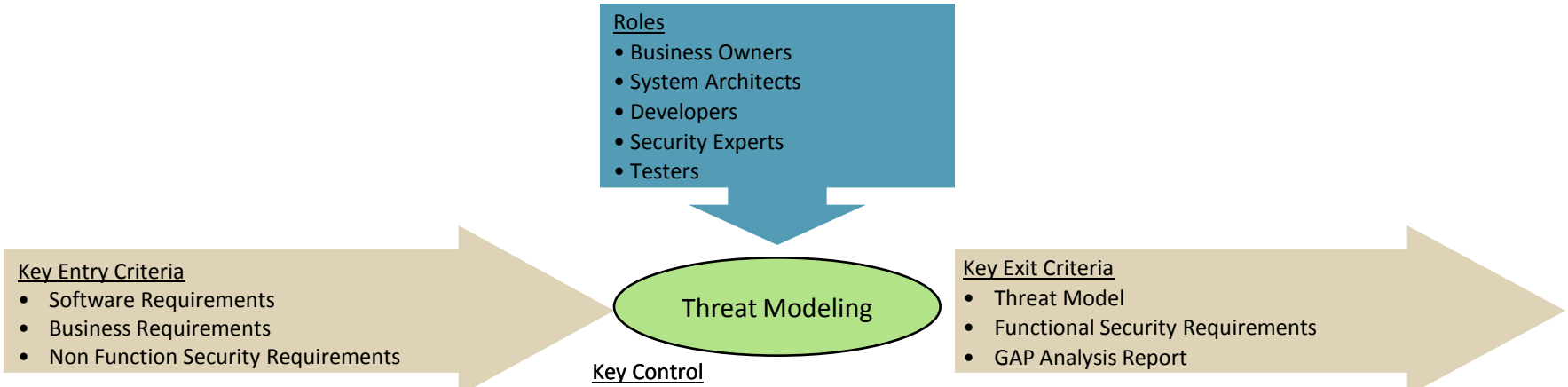
What is Microsoft Application Threat Modeling?

http://go.microsoft.com/fwlink?linkid=77002

ACE TEAM
SECURITY.
PRIVACY.
PERFORMANCE.

Threat Modeling

- The process of proactive identification and enumeration of threats to an application



Activities and Role Participation		
Security Design Requirements	▪ This activity primarily focuses on creating the security architecture of the system	▪ System Architects 100%
Threat Modeling	• Threat modeling allows system security personnel to communicate the potential damage of security flaws and prioritize remediation efforts	▪ Business Owners 10% ▪ System Architects 30% ▪ Developers 30% ▪ Security Experts 20% ▪ Testers 10%
Security Design Review	▪ A security design review aims to find any gaps in the design of an application from a secure by design prospective	▪ Security Experts 100%

Kung Fu 1: Proactive Security

Purpose

- Proactive approaches save $$ & time

Reason

- Design flaws identified early in lifecycle
- Focus on business rules rather than technical implementation

Advantages of TM

- Build security into plan rather than being reactive

Example

- Evaluating feature set at ISV

Kung Fu 2: Due Diligence

Purpose

- Compliance is among top CSO/CIO priorities
- Corporate security spend maps to compliance concerns

Reason

- No one wants to set the precedence for non-compliance
- Most tangibly quantifiable downside

Advantages of TM

- Documented security plan
- Ahead of the curve

Example

- Hospital CISO demonstrated due diligence to board after attack

Kung Fu 3: Competitive Differentiator

Purpose	• Security becoming increasingly relevant in competitive situations
Reason	• Clients want solution secure by design • Reduce risk profile from app portfolio
Advantages of TM	• Demonstrate sophistication of approach • Clearly documented roadmap& standards
Example	• Utility RFP process re-engineered to evaluate vendor security maturity

Kung Fu 4: Security Process Agility

Purpose

- Security comes from incremental changes
- Most organizations struggle with setting a security mindset

Reason

- Culture change is difficult
- Standards and best practices keep changing
- Education is difficult and has lag

Advantages of TM

- Changes to best practice can percolate down
- Teams have just in time info

Example

- Microsoft IT Business Units use TM to drive change

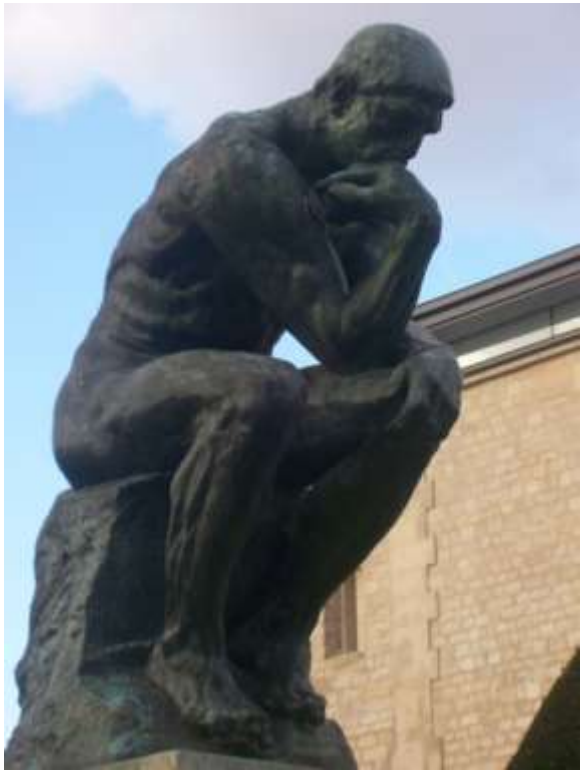
ACE Services

http://buildsecurityin.uscert.gov/daisy/bsi/resources/published/articles/932.html

http://blogs.msdn.com/ace_team

SECURITY. PRIVACY. PERFORMANCE

Lessons Learned



ACE TEAM SECURITY. PRIVACY. PERFORMANCE

http://en.wikipedia.org/wiki/Image:The_Thinker_close.jpg

Microsoft Solution Offerings

Consulting offerings

- Application Security
  - Security Code Reviews
  - Enterprise Threat Modeling
  - Security Guidance Development
  - Application Security Program development
  - Security Training – Threat Modeling/ Secure Application Dev
- Infrastructure Services
  - Technical Compliance Management using TCM tool
  - PKI, ISA, RMS security architecture/deployments
- Performance Services
  - Application Performance Testing
  - Building Performance Test Frameworks
  - Active Performance Monitoring

Conclusion

What did we talk about?

Proactive Security

Security Process Agility

Due Diligence

Competitive Differentiator

people ready

ACE TEAM SECURITY. PRIVACY. PERFORMANCE.

Contact

How do I find out more?

- Contact info for Microsoft ACE Services

  acesvc@microsoft.com

- Talk to your Microsoft Technical Account Manager or Services Executive
- Akshay blogs at:

http://blogs.msdn.com/akshay_aggarwal

http://noFUD.org