Security Architecture & Network Situational Awareness

September 27, 2016
Today’s web conference is generously sponsored by:

https://redseal.co/

The Measure of Resilience
Security Architecture & Network Situational Awareness

Welcome Conference Moderator

Mark Kadrich

- 25 Years in Information Security
- CISO at SDHC Health Exchange & CISO at 211 San Diego
Introduction

• All sound engineering begins with “principles”
  • What are you designing?
  • What is the expected outcome?
  • What are the performance parameters?
  • How will it fail?
  • Will it fail safely?
  • How will you test it to verify your assumptions?
  • How long will it be expected to last?
  • How will you expand or grow the architecture?
• Our present situation....
  • Most security “architectures” rely on chaos theory for requirements
    • What is the threat du jure?
    • What can our vendor provide?
    • Software has many and unpredictable failure modes
  • Budget versus user consensus usually rules the day
    • Look at BYOD policies!
    • How will you incorporate the next user driven technology wave?
• We need to move to an engineering driven approach to architecture
  • Documented desired behaviors
  • Model driven
  • Understood failure modes
  • Predictable results
  • Test, analyze, fix
  • Flexible, reliable, and stable
Today’s Speakers

Ben Tomhave, CISSP
• Security Architect with New Context
• Master of Science in Engineering Management

Jerry Sto. Tomas, CISSP, CISM
• CISO for Apria Healthcare
• Over 20 Years of IT, Privacy and Information Security Experience
Ben Tomhave

• Security Architect with New Context, a Lean Security Firm
• Previously held positions with Garner, AOL, Wells Fargo, ICSA Labs, LockPath and Ernst & Young
• Former co-chair of the American Bar Association Information Security Committee
• Holds a Masters in Science from George Washington University and is a CISSP
NEW CONTEXT

Something [Old, New, Borrowed, Blue, Lean]

Ben Tomhave, Security Architect

ISSA Webinar – Sept 2016
Something Old

Protect
Detect
Correct

Confidentiality
Availability
Integrity

Prepared for ISSA webinar participants.
## Something New

<table>
<thead>
<tr>
<th>Visibility</th>
<th>Control</th>
<th>Remediation</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IoT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• LAN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• WAN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Extranet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DIM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DAR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DIU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Apps</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Something Borrowed

- From Agile/DevOps
  - Systems Thinking
  - Amplify Feedback Loops
  - Culture of Continual Experimentation and Learning
  - Cooperative / Generative (vs Competitive)
  - Shared Values, Principles, Objectives, Risks, Tolerances, Language

- From Test-Driven Development
  - Define a test, THEN make a change, THEN evaluate for success/failure

- From Lean
  - Efficient
  - Effective
  - Knowledge-creating
  - Respectful & Mindful
  - Optimized Quality

Prepared for ISSA webinar participants.
Something Blue

• None of what we’ve discussed thus far matters...
  • ...in the current business environment

• Problem State...

• Where we spend time:
  • Justifying our existence
  • Fighting a perverse incentive model
  • Fighting against org culture
The goal of the Lean Security model is to transform how the business functions.
Awareness

- Communication
  - Openness
  - Clarity
  - Integrity
- Collaboration
  - Shared Tools / Platforms
  - Cooperative Spirit
  - Generative Culture
- Discoverability
  - Documentation
  - Networking (human, not IT)
  - Training
Execution

• Lean
  • Efficient
  • Effective
  • Knowledge-creating
  • Respectful & Mindful
  • Optimized Quality

• Test-Driven

• Dev(Sec)Ops
  • Systems Thinking
  • Amplify Feedback Loops
  • Culture of Continual Experimentation and Learning
  • Cooperative/Generative (vs Competitive)
  • Shared Values, Principles, Objectives, Risks, Tolerances

Prepared for ISSA webinar participants.
Measurement

• Means
• Method
• Motivation
  • Meaningful!

For example...
• Mean time to detection
• Mean time to response
• Mean time to recovery
• Mean time to remediation
Simplification

• Find lowest common denominator
• If too complex, (re)factor, find a better approach
• When all else fails, go back to Awareness and Execution
• Identify and address “undiscussable issues”
  • Topics that are uncomfortable, embarrassing, or may lead difficult conversations (e.g., “management is incompetent” or “won’t do any good anyway” or “fear of repercussions”) – people are actively chatting about them everywhere, but not the right people (meaning, not those who can institute changes)
  • Engage people at all levels in order to generate energy to promote change
  • Key in triggering turning points
• Find ways to break silos, take systemic view

Prepared for ISSA webinar participants.
Automation

• What can be automated?
  • Builds, Deployments, Maintenance (CI/CD)
  • Workflows
  • Provisioning

• What can’t be automated?
  • Why not?
    • Human as fail-safe
    • Trust issues: real or imagined/manufactured?

• Ops/Tech/Process maturity
  • e.g., if we move to a cloud-first strategy, can we actually support that and do it “right” without harming the business?
Closing Thoughts

• We cannot be successful in the current climate...
  • ...at least, not without *cultural* change!

• Technology is *an* answer, but not *the* answer.

• Security architecture must derive from business needs.

• First solve for communication, collaboration, and *cooperation*...
  • ...*then* have tool discussions.

• After Awareness: Execution, Measurement, Simplification, Automation
  • SecArch derives from all 5 principles of Lean Security

Ben Tomhave
ben.tomhave@newcontext.com
www.newcontext.com
Jerry Sto. Tomas

- CISO for Apria Healthcare
- Holds a Master’s Degree in Information Assurance from Norwich University
- Formerly held positions with Allergan, The Impac Companies and Celestica, Inc.
- Certifications include CISSP and CISM
Traditional Security Triad

Confidentiality

Integrity

Availability
Security Quad

Confidentiality
Integrity
Availability

Confidentiality
Integrity
Availability
Safety

Increasing risks as technology evolves

ISSA
Security Architecture & Network Situational Awareness
Stop Sign and Security

- Technology Trends
  - Big Data, Cloud, Mobility, Social, IoT
- Does your business think of you as a stop sign?
- Change security architecture to business enabler
  - Agile
  - Competitive
  - Compliant
## Traditional “Defense in Depth”

<table>
<thead>
<tr>
<th>Prevention Technologies</th>
<th>Detection Technologies</th>
<th>Response Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Anti-virus</td>
<td>• Intrusion Detection System</td>
<td>• Forensics &amp; Investigations</td>
</tr>
<tr>
<td>• Anti-spam</td>
<td>• Vulnerability Scanners</td>
<td>• Intelligence</td>
</tr>
<tr>
<td>• Endpoint encryption</td>
<td>• Event Collection &amp; Correlation</td>
<td>• Patch Management</td>
</tr>
<tr>
<td>• Firewalls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mobile Device Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DLP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Identity and Access Mgt.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Traditional “Defense in Depth” Approach

- “Checkbox” Mentality
  - Anti-virus, NGFW, DLP, etc.
- Difficulty to identify root-cause
  - People, Process, or Technology
- Value measurement
- Lack of correlated threats across the organization
Adaptive and Risk-based Security Architecture & Network Situational Awareness

Correlate and Predict

Situational Awareness and Sustainable Operations...
Holistic View: Sec Ops

**THREAT INTELLIGENCE**
- Cyber Risk Intelligence (e.g., Internet, Social Media)
- 3rd Party Security Intelligence Feeds (e.g., CERT, NIST, SANS, NH-ISAC)
- Security Product Alerts
- Security Analytics

**INCIDENT MANAGEMENT**
- Data Loss/Leakage (DLP)
- Advanced Persistent Threats
- Virus Attacks
- Email Spam Penetrations
- Network Intrusions
- System Hacking
- Web Defacement
- Denial-of-Service Attacks

**TECHNOLOGY MANAGEMENT**
- Perimeter Control (e.g., Firewall, Intrusion Prevention System, Anti-Spam, Web Content Filter)
- Endpoint Security (e.g., Anti-Virus, Mobile Device Mgt., DLP, Encryption)
- Identity and Access
- Patch Management
- Cloud Security Controls
- Vulnerability Scanners
Holistic View: Sec Ops

INCIDENT MANAGEMENT
- Data Loss/Leakage (DLP)
- Advanced Persistent Threats
- Virus Attacks
- Email Spam Penetrations
- Network Intrusions
- System Hacking
- Web Defacement
- Denial-of-Service Attacks

THREAT INTELLIGENCE
- Cyber Risk Intelligence (e.g., Internet, Social Media)
- 3rd Party Security Intelligence Feeds (e.g., CERT, NIST, SANS, NH-ISAC)
- Security Product Alerts
- Security Analytics

TECHNOLOGY MANAGEMENT
- Perimeter Control (e.g., Firewall, Intrusion Prevention System, Anti-Spam, Web Content Filter)
- Endpoint Security (e.g., Anti-Virus, Mobile Device Mgt., DLP, Encryption)
- Identity and Access
- Patch Management
- Cloud Security Controls
- **Vulnerability Assessment Scanners**
Situational Awareness: VA Scanners

- Scanners are managed within a Vulnerability Management program
- Security Analytics provide prioritization of remediation
- Helps IT to be a threat-aware organization
Situational Awareness: VA Scanners

Network Engineers: Access & Policy
- Config Mgt.

CIO/CISO
Policy/Compliance
- Exec
- Dashboards

Security Engineers: Prioritization & Speed
- Patch Mgt.
- Vuln Mgt.

Security Analytics

UI & API

- Firewalls
- Routers
- Load Balancers
- Switches
- SDN
- SIEM
- Scanners
- Endpoint
Situational Awareness: Network Zones

- Network visibility to analyze and monitor threats on each segment (e.g., Internet/Web DMZ, Application DMZ, Database zone, Internal server, User zone)
- Security Analytics provide a view of all segments and access path
- Helps identify direct attack path
Situational Awareness: Network Zones

- No access to Critical Assets or untrusted
- Approved, planned access
- Vulnerabilities are accessible from untrusted over unauthorized path.
Adaptive Model Vision

“I need to understand and accurately config my network”
Network/Network Sec Engineers

“I need to define and enforce access policies”
Network/Security Architects

“I need to prioritize and remediate vulnerabilities with limited resources”
Vulnerability Management/Sec Ops

“I need to identify and quickly respond to Incidents”
Sec Ops

Network Management & Devices
- CISCO
- HP

Platforms
- VMware
- NSX
- openstack
- Amazon web services

Vulnerability Managers
- Qualys
- Tripwire
- IP360
- Rapid7
- BeyondTrust
- Tenable

SIEM
- HP ArcSight
- Splunk
- IBM
- SolarWinds

Holistic View
- Analytics
  - RedSeal
- Ticketing
  - Remedy
- Workflow
- Inventory
  - ServiceNow
  - SolarWinds
Benefits of an Adaptive Model

Security Strategy That Is

- Resilient
- Risk Tolerant
- Meaningful Metrics
In summary...

- Adaptive and Risk-based
- Situational Awareness
- Predictability
Open Discussion & Q&A

- Mark Kadrich - Moderator
- Ben Tomhave
- Jerry Sto. Tomas

To ask a question:
Type in your question in the Questions area of your screen.

You may need to click on the double arrows to open this function.

#ISSAWebConf
We thank today’s sponsor:

https://redseal.co/

The Measure of Resilience
Upcoming ISSA International Web Conference

How to Recruit and Retain Cybersecurity Professionals

2-Hour Live Event: Tuesday, October 25, 2016
Start Time: 9:00 a.m. US-Pacific/ 12:00 p.m. US-Eastern/ 5:00 p.m. London
A recording of the conference and a link to the survey to get CPE credit for attending the August ISSA International Web Conference will soon be available at:

If you or your company are interested in becoming a sponsor for the monthly ISSA International Web Conferences, please visit: https://www.issa.org/?page=BecomeASponsor