Enterprise Security

Advanced Threat Detection & Response

Bert Hayes
Agenda

- Agenda
- Introduction
- Security Program Critical Path
- Collecting Data to identify breaches
- Incident Response
Bert Hayes

- Senior Solutions Engineer: Splunk, Inc.  2013 – Today
- bert@splunk.com
- Network Security Analyst
- Digital Forensics & Incident Response
  - Public Sector Focused
    - Texas Education Agency
    - University of Texas at Austin
    - Texas Department of Information Resources
    - Texas Higher Education Coordinating Board
CYBER CRIMINALS

MALICIOUS INSIDERS

NATION STATES
Advanced Threats Are Hard to Find

- Cyber Criminals
- Nation States
- Insider Threats

- 100% Valid credentials were used
- 40 Average # of systems accessed
- 229 Median # of days before detection
- 67% Of victims were notified by external entity

All Data is Security Relevant = Big Data

- Threat Intelligence
- Email
- Web
- Desktops
- Servers
- DHCP/DNS
- CMDB
- Hypervisor
- Badges
- Storage
- Mobile
- Firewall
- Authentication
- Vulnerability Scans
- Intrusion Detection
- Data Loss Prevention
- Anti-Malware
- Custom Apps
- Network Flows
- Physical Access
- Transaction Records
Security Program: The Big Picture
Security Program: The Big Picture

It’s complicated...
Three Interrelated Components of Security

- Process
- Technology
- People
But which is most important?

1. People

Process

Technology
Then what?

1. People

2. Process

Technology
A Security Program

Information Security Program

- Security Program Management
- Business Continuity and Disaster Recovery
- Business and Technology Enablement
- Identity and Access Management
- Legal and Human Resources

Operational Critical Path
- Governance, Risk, Compliance
- Security Architecture
- Security Engineering
- Security Operations
- Security Community Outreach
Security Critical Path

- Risk & Compliance
- Security Operations (Includes SOC)
- Security Architecture
- Security Engineering
Security Critical Path

Risk and Compliance

- Asset identification
- Risk
  - Assets
  - Threats (Actors, Actions, Modeling)
  - Vulnerabilities (Vulnerability management)
- Compliance
- **Outcome: Prioritized list of what to protect**
Security Critical Path

Threats

- An extremely important topic of discussion
- Threat: A person, group, or thing likely to damage or endanger
  - Internal: Malicious insider, whistleblower, clueless insider
  - External: Nation states, organized crime, hacktivists, script kiddies
- Use Microsoft’s STRIDE model to generate conversational questions:
  - Spoofing (identity)
  - Tampering
  - Repudiation (proof)
  - Information Disclosure
  - Denial of Service
  - Elevation of Privilege
## Security Critical Path

### Threat Actions and Threat Actors

<table>
<thead>
<tr>
<th>CRIMEWARE</th>
<th>CYBER-ESPIONAGE</th>
<th>DENIAL OF SERVICE</th>
<th>PHYSICAL THEFT/LOSS</th>
<th>MISCELLANEOUS ERRORS</th>
<th>PAYMENT CARD SKIMMERS</th>
<th>POINT OF SALE</th>
<th>INSIDER MISUSE</th>
<th>WEB APP ATTACKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>73%</td>
<td>5%</td>
<td>31%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>61%</td>
</tr>
<tr>
<td>97%</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6%</td>
</tr>
<tr>
<td>41%</td>
<td>6%</td>
<td>18%</td>
<td>5%</td>
<td>6%</td>
<td>2%</td>
<td>1%</td>
<td>3%</td>
<td>3%</td>
</tr>
</tbody>
</table>

**Source:** Verizon DBIR 2015
## Security Critical Path

### Threat Actions and Industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cyber-espionage</th>
<th>Denial of Service</th>
<th>Physical Theft/Loss</th>
<th>Miscellaneous Errors</th>
<th>Payment Card/Data</th>
<th>Point of Sale</th>
<th>Insider Misuse</th>
<th>Web App Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educational</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mining</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Verizon DBIR 2015
Security Critical Path

Threats and Vulnerabilities

- Can an organization completely prepare for every threat?
  - No!
- Can an organization completely eliminate every vulnerability?
  - No!
- So where should an organization start?
  - By applying Risk Analysis
Security Critical Path

Risk

- Risk is an often misunderstood concept and term
- From a conversational perspective, think of risk like this
  - Risk = Likelihood X Impact
  - Risk = Threats X Vulnerabilities
- Significant Risk only exists with the potential for significant Loss
- If done properly, risk can (and should) be measured in monetary terms, literally: $ £ €
- Risk frameworks to know:
  - Annualized Loss Expectancy (ALE) to be used as a counter-example (and to pass the CISSP exam!)
  - Factor Analysis of Information RISK (FAIR)
Security Critical Path

Risk Treatment

• Once risk has been identified, it must be dealt with
  • Avoid
  • Reduce
  • Transfer
  • Accept
Security Critical Path

Compliance

- Compliance is often prescriptive, not driven purely by risk analysis
- Controls and activities that do not effectively lower security risk are sometimes required
- If an organization does not have an experienced security team, sometimes compliance is more prominent than risk management
- Compliance is driven by
  - Region
  - Industry/vertical
  - Activities (Credit card processing, etc.)

Compliance can be just as important as Risk as a driver for future phases in the security critical path.
Security Critical Path

Security Architecture

- Control Selection / Design
  - Defense in depth
  - CIS (SANS) 20 Critical Controls
  - ISO/IEC 27002
- Controls are also known as **countermeasures**
- Cost of the countermeasure should be less than the risk facing the organization
- Network security and monitoring architecture
- Interface with other teams
- **Outcome:** What controls will be implemented, and where
Adversary Perspective - Attack Kill Chain

Reconnaissance | Delivery | Installation | Actions on Objectives

Weaponization | Exploitation | Command and Control (C2)

Gartner’s Five Styles of APT Defense
Security Critical Path

Security Engineering

- Implement controls
- Maintain security systems, responsible for uptime
- Change management is important
- Operational visibility for security systems
- **Outcome:** Stable platform for security operations
Security Critical Path

Security Operations

- Operational security capability
  - Prevent
  - Detect (includes hunting!)
  - Respond
- This is where the Security Operation Center (SOC) lives!
- **Outcome: Consistent, repeatable, measurable security response capability**
Get the how-to

Crafting the InfoSec Playbook

Jeff Bollinger, Brandon Enright & Matthew Valites
The Ever-changing Threat Landscape

- **100%** Valid credentials were used
- **67%** Victims notified by external entity
- **229** Median # of days before detection

Data Sources Required

- Network
- Endpoint
- Threat Intelligence
- Access/Identity
Data Sources Required

- **Threat intelligence**
  - 3rd party Threat Intel
  - Open source blacklist
  - Internal threat intelligence

- **Network**
  - Firewall, IDS, IPS
  - DNS
  - Email
  - Web Proxy
  - NetFlow
  - Network

- **Endpoint**
  - AV/IPS/FW
  - Malware detection
  - Config Management
  - Performance
  - OS logs
  - File System

- **Access/Identity**
  - Directory Services
  - Asset Mgmt
  - Authentication Logs
  - Application Services
  - VPN, SSO

- Known relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution
- Who talked to whom, traffic, malware download/delivery, C2, exfiltration, lateral movement
- Running process, services, process owner, registry mods, file system changes, patching level, network connections by process/service
- Access level, privileged use/escalation, system ownership, user/system/service business criticality
Examples of What’s Available From the Streaming Network/Wire Data

<table>
<thead>
<tr>
<th>Performance Metrics</th>
<th>Application Data</th>
<th>Business Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round Trip Time</td>
<td>POST Content</td>
<td>Product ID</td>
</tr>
<tr>
<td>Client Request Time</td>
<td>AJAX Data</td>
<td>Customer ID</td>
</tr>
<tr>
<td>Server Reply Time</td>
<td>Section</td>
<td>Shopping Cart ID</td>
</tr>
<tr>
<td>Server Send Time</td>
<td>Sub-Section</td>
<td>Cart Items</td>
</tr>
<tr>
<td>Total Time Taken</td>
<td>Page Title</td>
<td>Cart Values</td>
</tr>
<tr>
<td>Base HTML Load Time</td>
<td>Session Cookie</td>
<td>Discounts</td>
</tr>
<tr>
<td>Page Content Load Time</td>
<td>Proxied IP Address</td>
<td>Order ID</td>
</tr>
<tr>
<td>Total Page Load Time</td>
<td>Error Message</td>
<td>Abandoned?</td>
</tr>
</tbody>
</table>
Capabilities - Scoping Infections and Breach

Connecting Data and People

Analytics

Context & Intelligence
Exploitation != GameOver
Best Practices – Breach Response Posture

- Bring in data from (minimum at least one from each category):
  - Network – next gen firewall or web proxy, email, dns
  - Endpoint – windows logs, registry changes, file changes
  - Threat Intelligence – open source or subscription based
  - Access and Identity – authentication events, machine-user mapping

- Employ a security intelligence platform so analysts can:
  - Contextualize events, analytics and alerts
  - Automate their analysis and exploration
  - Share techniques and results to learn and improve
Kill Chain – Breach Example

Delivery
Exploitation
Installation
C2 Actions on Objectives

Attacker creates malware, embed in .pdf, emails to the target

Remote control
Steal data
Persist in company
Rent as botnet

http (web) session to command & control server

.pdf executes & unpacks malware
overwriting and running "allowed" programs

Read email, open attachment

Threat intelligence
Network
Endpoint
Access/Identity
Breach Example – Disruption Opportunities

Delivery  Exploitation  Installation  C2  Actions on Objectives

Threat intelligence
Network
Endpoint
Access/Identity

Attacker creates malware, embed in .pdf, emails to the target
Read email, open attachment
.http (web) session to command & control server
.pdf executes & unpacks malware overwriting and running "allowed" programs

Remote control
Steal data
Persist in company
Rent as botnet

MAIL
WEB

Aracker creates malware, embed in .pdf, emails to the target
MAIL
WEB

Read email, open attachment

.pdf executes & unpacks malware overwriting and running "allowed" programs

Remote control
Steal data
Persist in company
Rent as botnet

WEB
Job Continues – Need to Perform Incident Investigation
Use Multiple Data Sources to Link Events
Advanced Threat Detection & Response

Transaction

Gain Access to system

Create additional environment

Conduct Business

Threat intelligence

Network Activity/Security

Host Activity/Security

Auth - User Roles, Corp Context

Events that contain link to file

What created the program/process?

How was process started?

Process making C2 traffic

Proxy log C2 communication to blacklist

Web Portal

MAIL

WEB

.sdf

Calc.exe

Svchost.exe

.sdf

.Web Portal
Connect the “Data-Dots” to See the Whole Story

<table>
<thead>
<tr>
<th>Delivery, Exploit Installation</th>
<th>Gain Trusted Access</th>
<th>Upgrade (escalate) Lateral movement</th>
<th>Data Gathering</th>
<th>Exfiltration</th>
<th>Persist, Repeat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Attacker, know relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Activity/Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Where they went to, who talked to whom, attack transmitted, abnormal traffic, malware download</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Activity/Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What process is running (malicious, abnormal, etc.) Process owner, registry mods, attack/malware artifacts, patching level, attack susceptibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth - User Roles, Corp Context</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Access level, privileged users, likelihood of infection, where they might be in kill chain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Third-party Threat Intel
- Open source blacklist
- Internal threat intelligence

- Firewall
- IDS / IPS
- Vulnerability scanners
- Web Proxy
- NetFlow
- Network

- Endpoint (AV/IPS/FW)
- Malware detection
- PCLM
- DHCP
- OS logs
- Patching

- Active Directory
- LDAP
- CMDB
- Operating System
- Database
- VPN, AAA, SSO
Connect the “Data-Dots” to See the Whole Story

1. Threat Intelligence Data
2. Email Data
3. Host or ETDR Data
4. Identity Data
5. Command & Control
6. Web or Firewall Data
7. Accomplish Mission
8. Threat Intelligence Data

Threat intelligence
Network Activity/Security
Host Activity/Security
Auth - User Roles, Corp Context

Identity, Roles, Privileges, Location, Behavior, Risk, Audit scope, Classification, etc.
Threat intelligence

Auth - User Roles, Corp Context

Network Activity/Security

Host Activity/Security

Start Anywhere, Analyze Up-Down-Across-Backwards-Forward

Delivery

Exploitation & Installation

Command & Control

Accomplish Mission

• Third-Party Threat Intel
  • Open source blacklist
  • Internal threat intelligence

• Firewall
  • IDS / IPS
  • Vulnerability scanners
  • Web Proxy
  • NetFlow
  • Network

• Endpoint (AV/IPS/FW)
  • Malware detection
  • PCLM
  • DHCP
  • OS logs
  • Patching

• Active Directory
  • LDAP
  • CMDB
  • Operating System
  • Database
  • VPN, AAA, SSO

Identity, Roles, Privileges, Location, Behavior, Risk, Audit scope, Classification, etc.
Thank You
Rapid Ascent in the Gartner SIEM Magic Quadrant*

2015 Leader and the only vendor to improve its visionary position
2014 Leader
2013 Leader
2012 Challenger
2011 Niche Player

*Gartner, Inc., SIEM Magic Quadrant 2011-2015. Gartner does not endorse any vendor, product or service depicted in its research publication and not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Industry Accolades

Best SIEM Solution

Best Enterprise Security Solution

Best SIEM
Thriving Community

- 800+ apps
- 40,000+ questions and answers
- Local User Groups and SplunkLive! events
- Dev.splunk.com