Security Monitoring in the Real World with Petabytes of Data

Mike Mellor
Outline

- About Mike
- About Adobe
- DMa environment
  - size of business, amount of hits/data we manage, fun facts, etc
  - Security operations program vs SPLC (why compliance alone isn't enough)
- New approach to security monitoring
- Threat intel
- Threat analytics
- Conclusion
About Me

- 6 years as Deputy Chief Information Security Officer (CISO) at major US Government agency
- Previously a senior security researcher at NIATEC
- Information Security exam developer for ISC(2)
- Currently in charge of security and compliance strategy for Adobe Marketing Cloud
- CIO for Utah Medical Outreach (non-profit)
Marketing Cloud Momentum: Verticals

- America’s largest financial services companies: 10/10
- World’s biggest auto companies: 10/10
- America’s top wealth management firms: 10/10
- World’s most valuable telecom brands: 10/10
- Adobe Marketing Cloud: 10/10
- World’s largest media companies: 9/10
- America’s largest corporations: 9/10
- World’s biggest hotel chains: 9/10
- World’s most valuable airlines: 8/10
- World’s top internet retailers: 7/10
- Highest revenue pharmaceutical companies: 6/10

Marketing Cloud at Scale in 2015

- **45.5T** Transactions
- **42PB** Dynamic Media Assets
- **750B** Target Transactions
- **7.9T** Analytics Transactions
- **5.5B** Impressions
- **5.3B** Active Profiles
- **139B** Primetime Transactions
- **100B** Emails
- **2M** Social Posts
- **2,700** customers on DTM
- **+98%** Assets Core Service
- **9X↑** Audiences Increase
- **42PB** Dynamic Media Assets
- **2M** Social Posts
- **5.5B** Impressions
- **5.3B** Active Profiles
- **45.5T** Transactions
- **750B** Target Transactions
- **139B** Primetime Transactions
- **7.9T** Analytics Transactions
- **100B** Emails
- **2,700** customers on DTM
- **+98%** Assets Core Service
- **9X↑** Audiences Increase
Our Mission:
Deliver a reliable, scalable, and secure customer experience across Adobe’s Enterprise cloud.
Our Priority for Hosted Services: Protect Customers and Their Data

Hosted Services

- Software
- Infrastructure
- Operations
- Physical

Secure Product Lifecycle

Security Certifications
Security Certifications: Common Controls Framework (CCF)

Started with 10+ standards, with a total of ~1000 Control Requirements (CRs)…. rationalized into ~ 200 common controls across 11 control domains tailored to Adobe’s Environment

- SOC 2 (5 Principles) – 116 CRs
- ISO 27001 – 26 CRs
- PCI DSS – 247 CRs
- FedRAMP - 325 CRs
- ISO 27002 – 114 CRs
- SOX 404 (IT) – 63 CRs

<table>
<thead>
<tr>
<th>Control Domain</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>12</td>
</tr>
<tr>
<td>Access Control</td>
<td>30</td>
</tr>
<tr>
<td>BCM</td>
<td>10</td>
</tr>
<tr>
<td>Cryptography</td>
<td>11</td>
</tr>
<tr>
<td>Data Privacy</td>
<td>10</td>
</tr>
<tr>
<td>Incident Response</td>
<td>6</td>
</tr>
<tr>
<td>Operations Management</td>
<td>70</td>
</tr>
<tr>
<td>Physical and Env. Security</td>
<td>16</td>
</tr>
<tr>
<td>People Resources</td>
<td>11</td>
</tr>
<tr>
<td>SDLC</td>
<td>11</td>
</tr>
<tr>
<td>Security Governance</td>
<td>31</td>
</tr>
</tbody>
</table>
Security Monitoring At Scale
Size and Scale Require a Novel Approach

- Spend $$$ on what matters
- Automation & workflow efficiency gains pay dividends
- Use open source where possible to enable better scalability
- Intelligence and technology
- Maximize the impact of resources
- Map to security compliance (business support and $$$)
- Math and security economics favor the attacker
Different Types of Data Are Needed

Network Security Monitoring
- NetFlow
- Actionable Data
- Application Layer (Bro)
- Full Packet Capture
- IDS (Suricata)

Host Security Monitoring
- File Integrity Monitoring
- Process Monitoring
- Actionable Data
- Command History
- IOC Searching
- File Integrity Monitoring
A “Big Data” Approach

- Centralize all data for rapid searching
- Use a hybrid analytics approach
- Use consolidated logging
- Log only what is needed and actionable
- Prioritize traffic
- Do not rely too heavily on public listening data
- Avoid large data flows that have no real actionable data
- Map data to severity alerts so it is actionable by teams
- Getting this right will require close coordination between engineering, monitoring, IR, and threat analytics teams
Good Threat Intelligence is Key to Security Program Maturity
Threat Intelligence Maturity Model

001  Basic security operations maturity

002  Not all Indicators of Compromise (IOC) are created equal

101  Pay vendors for threat intel (spoiler: this doesn’t work)

201  Collect & curate threat intel

301  Applied threat research
001 – Start here

- Data & environment
- Visibility at right places (constantly test)
- Right data in the right places
- Prioritize alerts by criticality, context, and multiple matches
  - Incoming traffic to webserver
  - Outgoing data (SSH/IRC/wget/curl)
  - Unique processes
  - Non-standard traffic (non-SSL on 443, etc)
- Threat intel
- Understand that 95% of breaches are not using 0 days
- Cyber security is hard – security economics favors the attackers
002 – Not all Indicators of Compromise (IOC) are created equal

Higher up pyramid value increases and difficulty/cost increases

Source: David Bianco, personal blog
101 – Paying Vendors for Threat Intel = FAIL

- Too many data points (internet minus 2 hosts)
- You need tight correlation with your own good data
- Context is key
- Most intrusions do not use obscure attacks
- Vendors that aid in removing noise are worth consideration
- There is no “magic list” you can buy
Each piece of threat intel has 1) value level and 2) shelf life

A smaller amount of "high value and fresh" threat intel is extremely valuable

- Curate the intel
- Keep the intel fresh
- Prioritize alerts by criticality, context, and multiple matches
- Focus on highest value systems
- Make interesting use of one-off projects that can collect less traditional intel
301 – Applied Threat Research (ATR)

- Research and apply TTPs from real world attackers
- Is attack successful against our systems?
- Did security monitoring detect the attack?
- DANGER! Extremely skilled security professionals required
- Almost all of your security program work should be focused on fixing issues found here – by far highest value
- ATR levels of ‘stealth’ – challenge and collaborate with security monitor team
- Auditors loves this – shows high degree of security.
Resources

- Security portal
  - http://adobe.com/security

- Security @ Adobe blog

- Advisories and updates
  - http://www.adobe.com/support/security

- Twitter: @AdobeSecurity
- Brad: @BradArkin