RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO1-T10

# Security Monitoring in the Real World with Petabytes of Data

**Mike Mellor**

Director, Information Security, Adobe

#RSAC

# The Adobe Advantage



Make Manage Measure Monetize

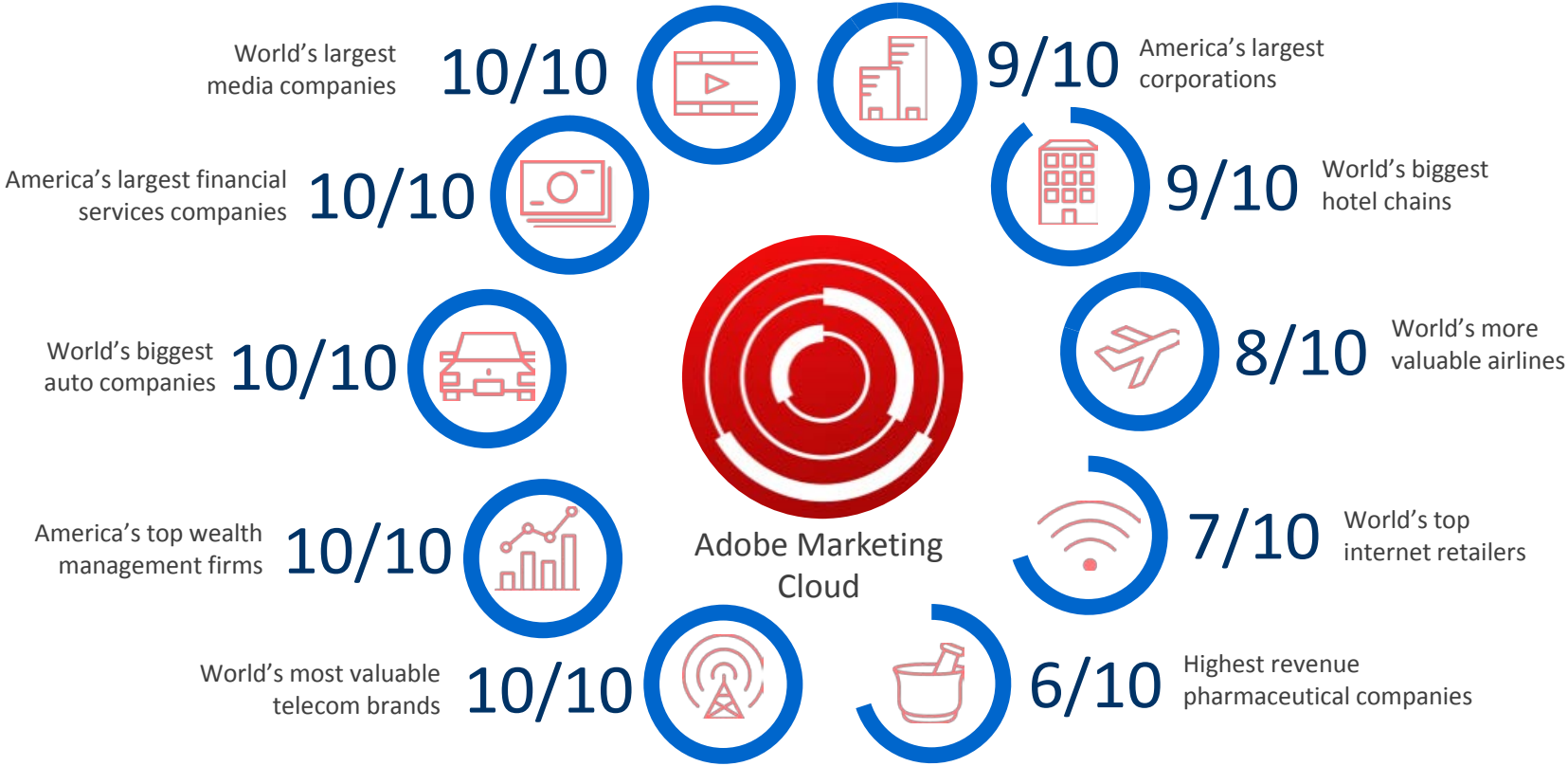
Adobe
Document Cloud

Adobe
Creative Cloud

Adobe
Marketing Cloud

# Broad Use Across Industries





# 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

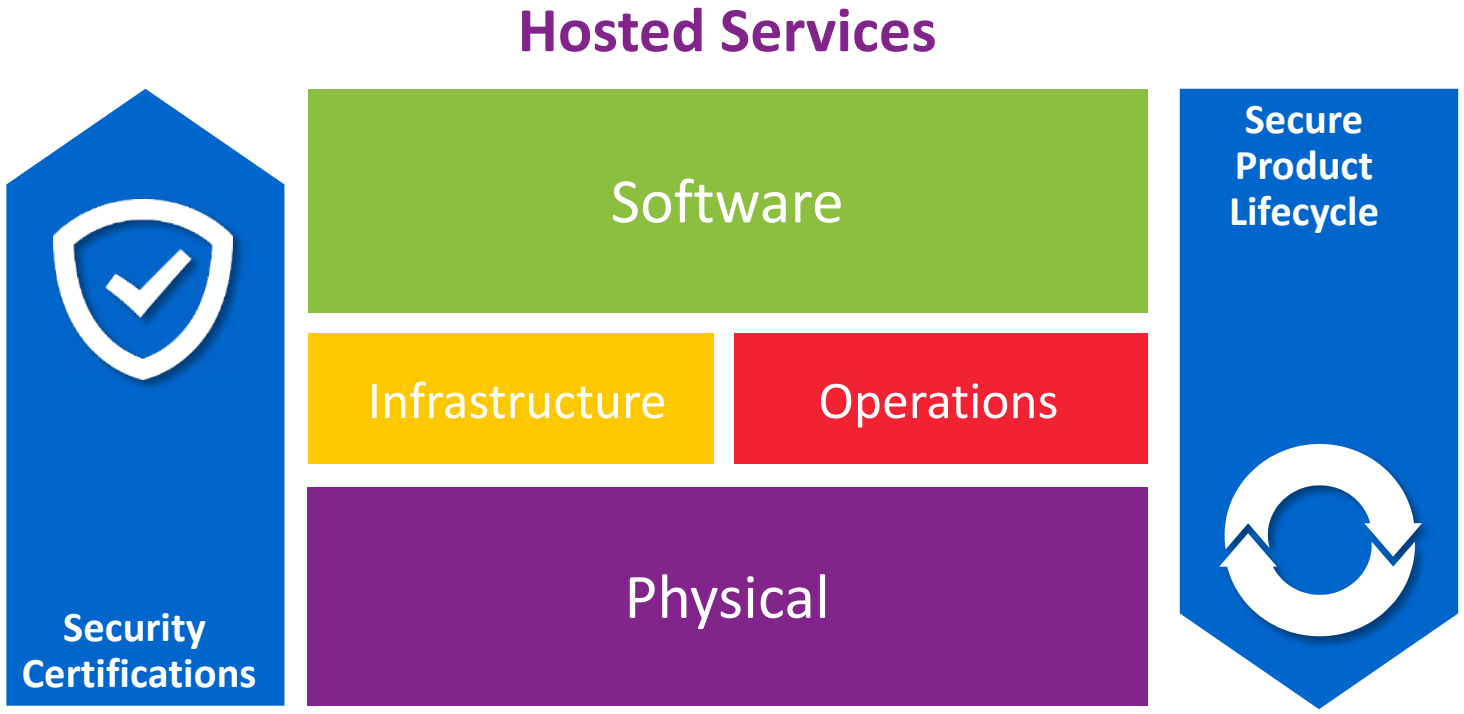
**+98%**
Assets Core Service

**9X↑**
Audiences Increase

In order to succeed we must deliver a **reliable**, **scalable**, and **secure** customer experience across Adobe's Enterprise cloud.

# The Priority for Hosted Services: Protect Customers and Their Data





# Security Certifications: Common Controls Framework (CCF)



Started with 10+ standards, with a total of ~1000 Control Requirements (CRs)....

SOC 2 (5 Principles) – 116 CRs
Service Organization Controls

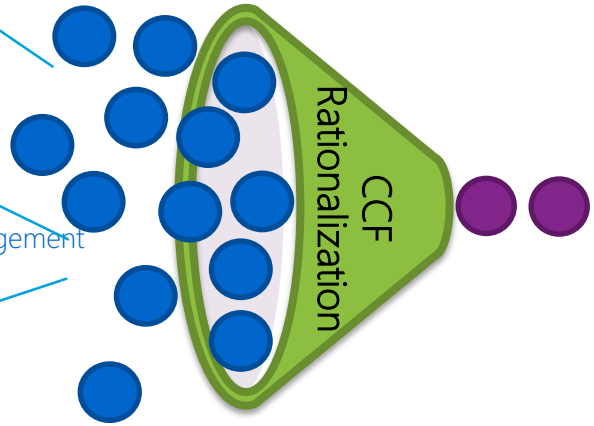
ISO 27001 – 26 CRs
International Organization for Standardization

PCI DSS – 247 CRs
Payment Card Industry - Data Security Standard

FedRAMP - 325 CRs
Federal Risk and Authorization Management Program

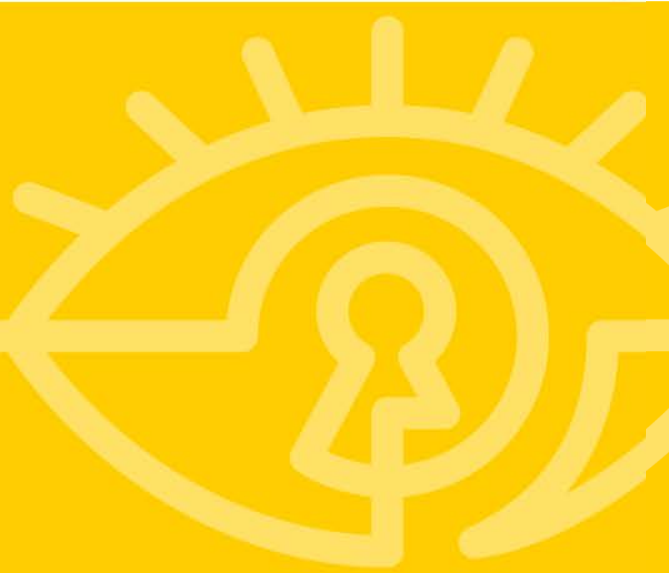
ISO 27002 – 114 CRs
International Organization for Standardization

SOX 404 (IT) – 63 CRs
Sarbanes Oxley 404




...rationalized into ~ 200 common controls across 11 control domains tailored to Adobe's Environment

- Asset Management - 12 Controls
- Access Control - 30 Controls
- BCM – 10 Controls
- Cryptography - 11 Controls
- Data Privacy - 10 Controls
- Incident Response- 6 Controls
- Operations Management - 70 Controls
- Physical and Env. Security - 16 Controls
- People Resources- 11 Controls
- SDLC – 11 Controls
- Security Governance - 31 Controls



# Security Monitoring At Scale

# Size and Scale Require a Novel Approach

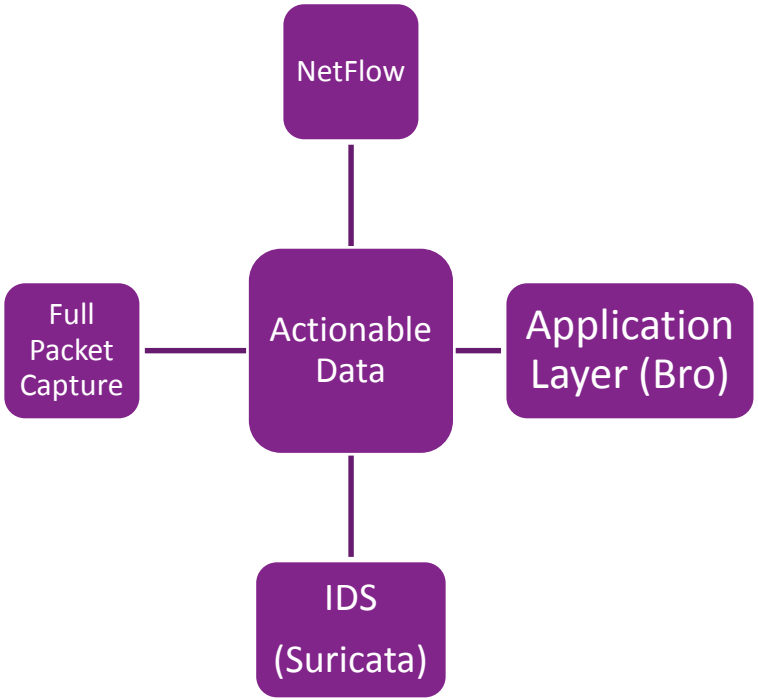


- Spend $$$ on what matters
- Automation & workflow efficiency gains pay dividends
- Use open source where possible to enable better scalability
- Intelligence and technology
- Maximize the impact of resources
- Map to security compliance (business support and $$$)
- Math and security economics favor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

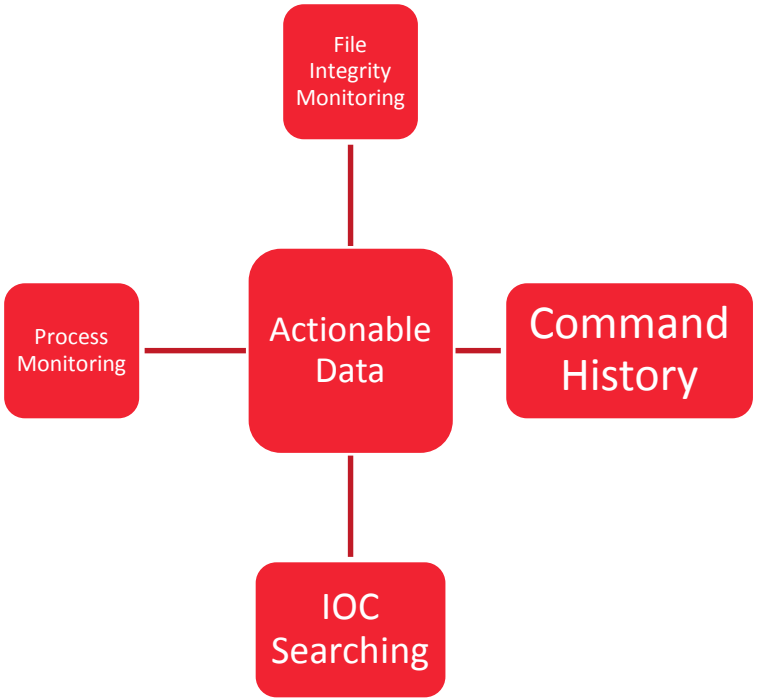
# Different Types of Data Are Needed



## Network Security Monitoring



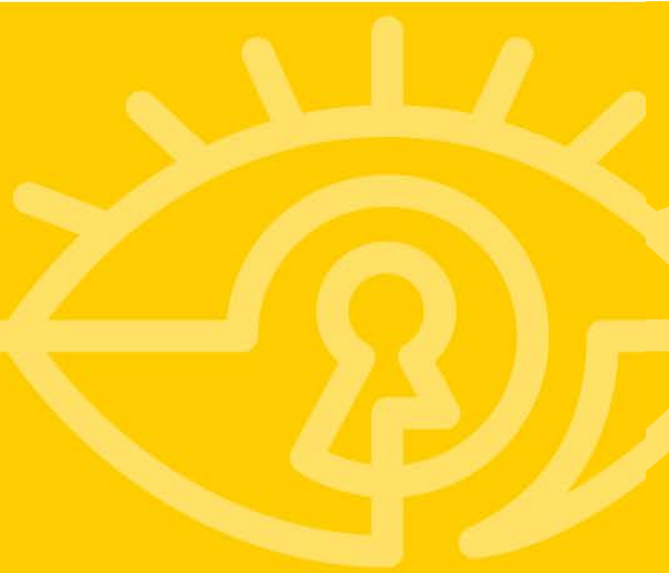

## Host Security Monitoring



# 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

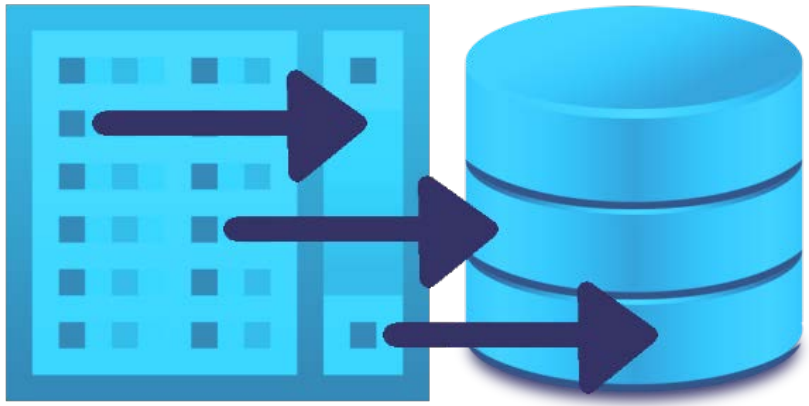


- **001** – Basic security operations maturity
- **002** – Not all Indicators of Compromise (IOC) are created equal
- **101** – Pay vendors for threat intel (spoiler: this doesn't work)
- **201** – Collect & curate threat intel
- **301** – Applied threat research

# 001 – Start here

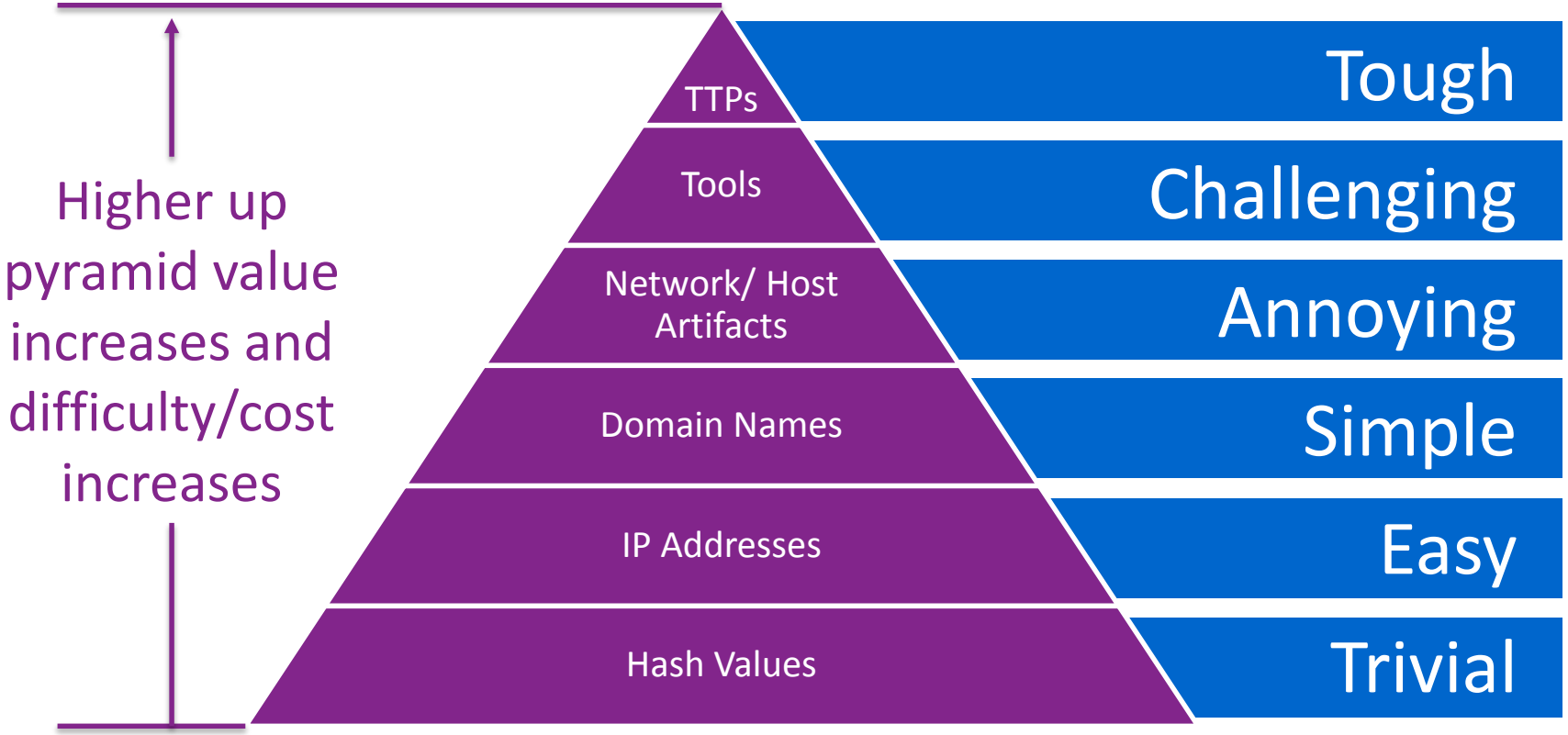


- Data & environment
- Visibility at right places (constantly test)
- Right data in the right places
- Prioritize alerts by criticality, context, and multiple matches
  - Incoming traffic to webserver
  - Outgoing data (SSH/IRC/wget/curl)
  - Unique processes
  - Non-standard traffic (non-SSL on 443, 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






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

# 201 – Collect & Curate Threat Intel



- 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 program maturity

# Conclusion

# Resources



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

- **Security @ Adobe blog**
- http:// blogs.adobe.com/security/

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

- **Twitter:** @AdobeSecurity
- **Brad:** @BradArkin

# Thank you