Ashley Madison: Cybersecurity in a World of Discretion

Matthew Maglieri | **ruby**

About the Speaker

Matthew Maglieri

CISO, **ruby**

- Ex-Mandiant - Red teamer, SOC transformation
- CISO @ **ruby** since January 2017
  - Parent company to Ashley Madison, amongst others
  - Based in Toronto, Canada
- Why am I here?

@matthewmaglieri linkedin.com/in/matthewmaglieri matthew.maglieri@rubylife.com

AM AND EM MUST SHUT DOWN
IMMEDIATELY PERMANENTLY
We are the Impact Team.
We have taken over all systems in your entire office and production domains,
all customer information databases, source code repositories, financial records, emails
Shutting down AM and EM will cost you, but non-compliance will cost you more:
We will release all customer records, profiles with all the customers' secret
sexual fantasies, nude pictures, and conversations and matching credit card
transactions, real names and addresses, and employee documents and emails.
Avid Life Media will be liable for fraud and extreme harm to millions of users.

“Build a leading privacy and information security program”

PCi

CERTIFIED
BY
RYERSON UNIVERSITY

NIST

FireEye

Deloitte.

EY
Building a better
working world

The Numbers Today

There was an average of

15,542

new member accounts opened each day in **2017**

On average there were

472,752

new monthly sign-ups in 2017

Full report: https://ashleymadison.com/2017report

Our Mission

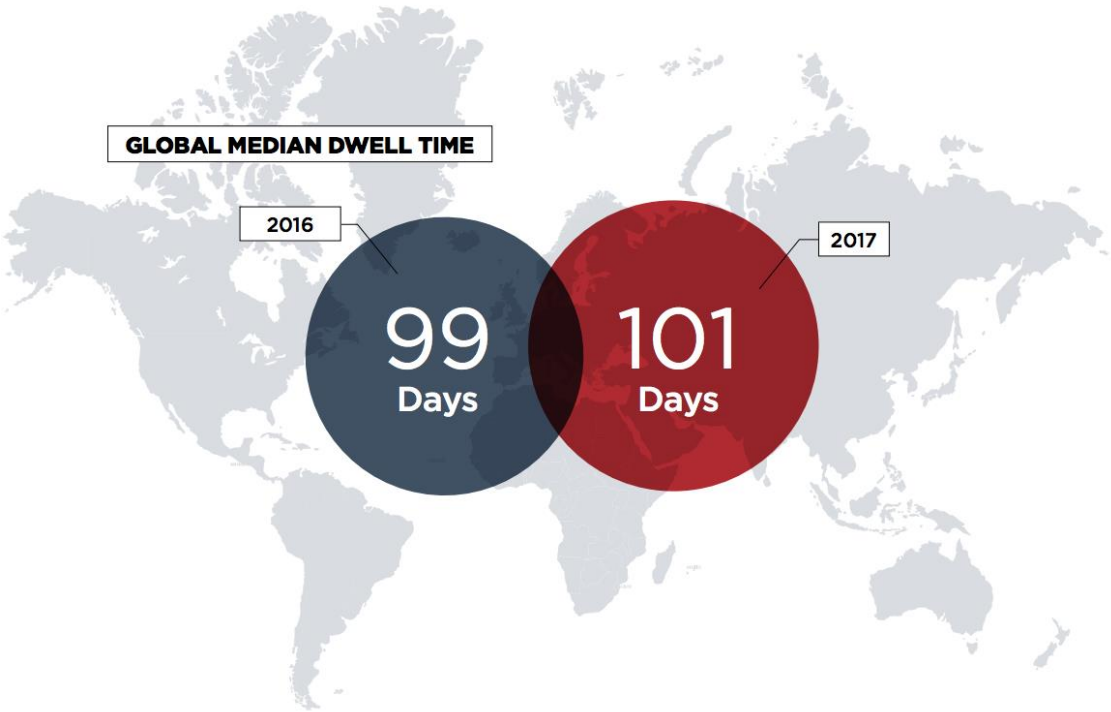
Build and maintain a leading threat-based, intelligence led information security program capable of defending ruby's systems, networks, and products from even the most advanced threats.

Breach Prevention, says Who?

Every week multiple breaches are publicly exposed, with many more kept private

It’s clear that our current approach as an industry is failing

Breach prevention likely isn’t possible, but achieving resilience is



Source: Mandiant M-Trends 2018

Why is our Approach as an Industry Failing?

"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."

– John Lambert, GM Microsoft Threat Intelligence Center

Defender Reality

The Fog of War

Attacker Reality

Find and exploit the weakest link

Pivot

Escalate privileges

Repeat

We Need to Evolve

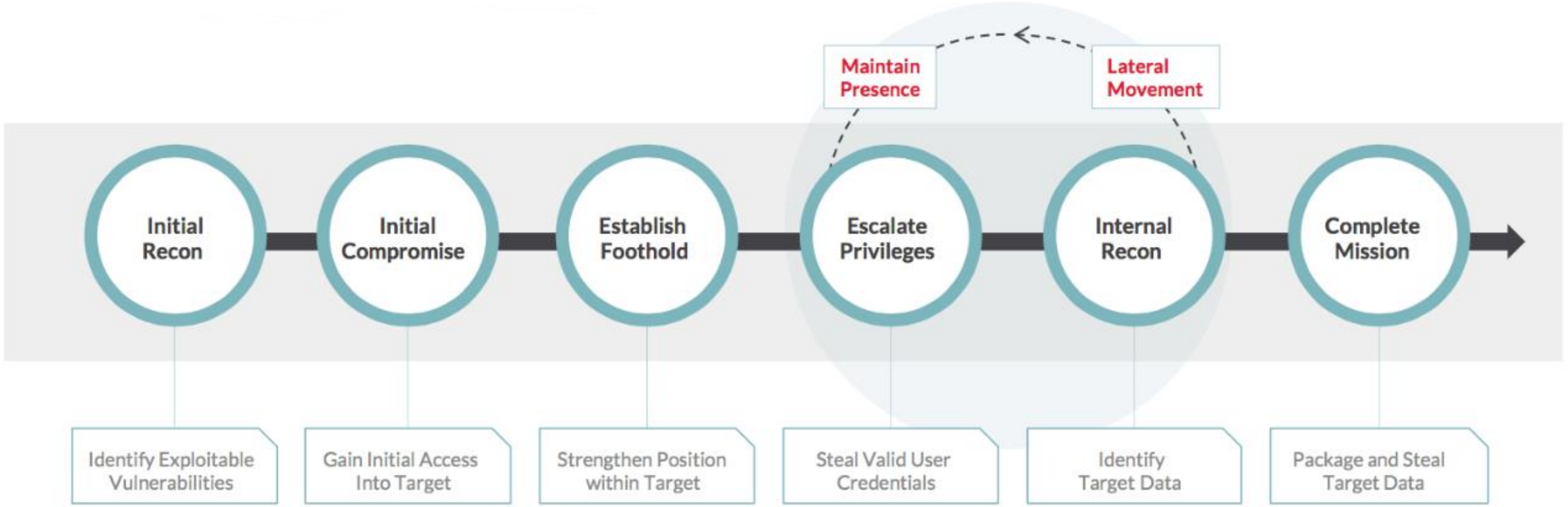
The old approach isn’t working

The threat landscape demands that we evolve and adapt

We’re building a connected world – we are the ones responsible for safeguarding and securing it

Offensive Risk Management

Need to understand the adversary and their TTPs

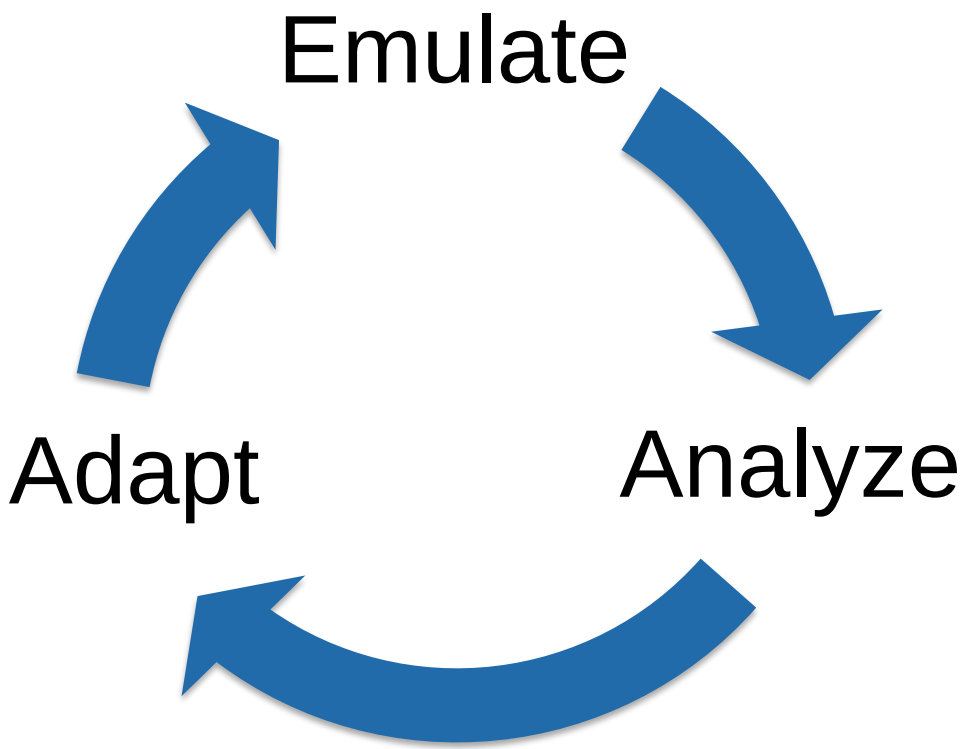


Mandiant targeted attack lifecycle

Offensive Risk Management

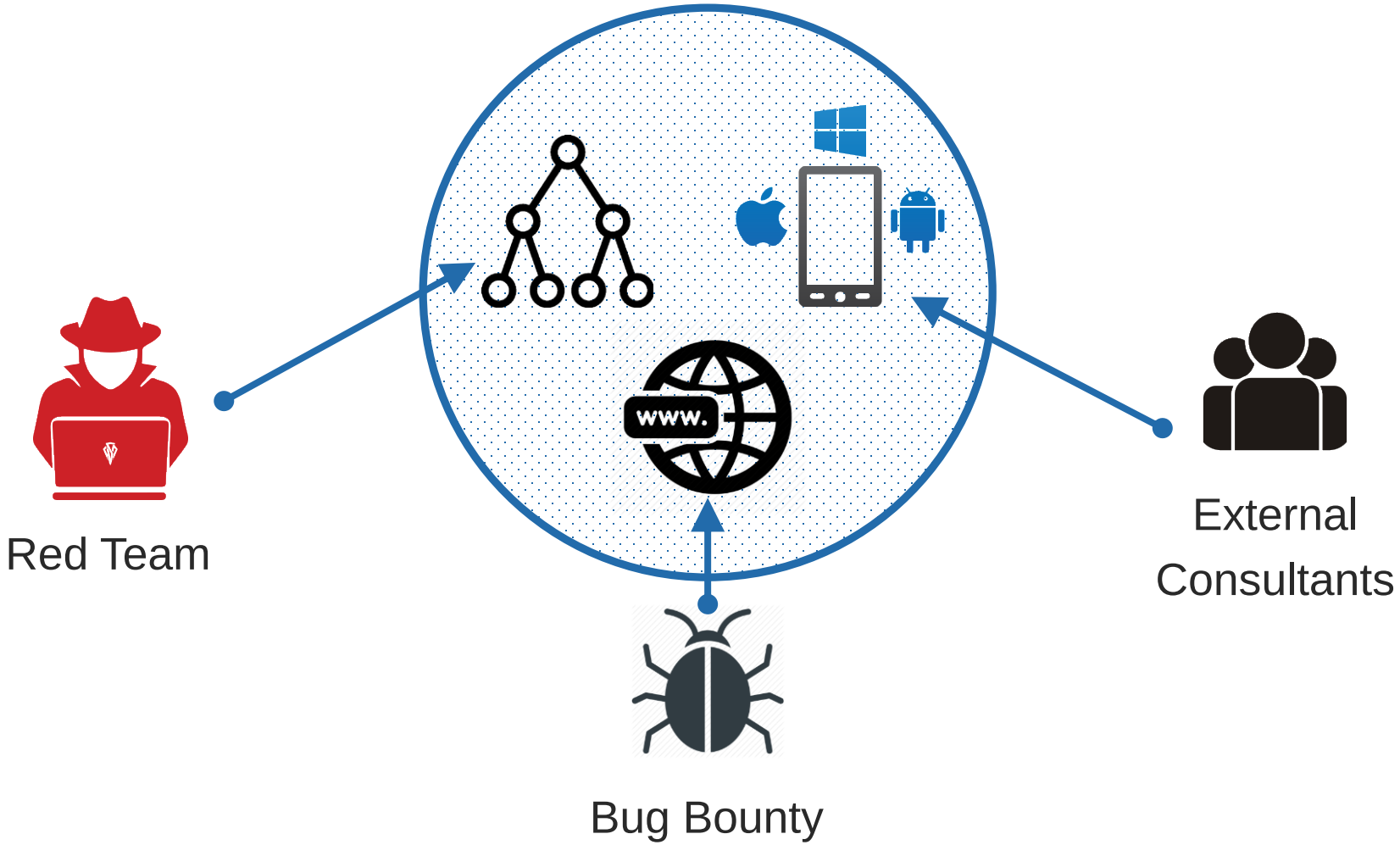
Emulate + Analyze + Adapt

Feed results into blue team (SOC) and security engineering (control enhancement, etc.)



Offensive Risk Management

Some part of your business should be under friendly attack at all times



Building a Resilient Environment

	Common Phase Activities	Example Controls
Initial Recon	▪ Open source intelligence (OSINT) gathering ▪ Passive and active port/service scanning	▪ Acceptable Use Policy (including guidelines on how to avoid revealing potentially sensitive corporate information online) ▪ Secure CDN/WAF ▪ Active and passive OSINT monitoring

Building a Resilient Environment

	Common Phase Activities	Example Controls
Initial Compromise	▪ Social engineering ▪ Vulnerability exploitation ▪ Internet-facing misconfiguration	▪ Email content filtering and anti-malware protection ▪ Security awareness and training program ▪ External vulnerability management ▪ Multi-factor authentication

Building a Resilient Environment

	Common Phase Activities	Example Controls
Establish Foothold	▪ Deploy malware ▪ Establish command and control ▪ Establish persistence	▪ Endpoint protection (anti-malware, anti-virus, live response, threat hunting) ▪ Network protection (content inspection, anti-malware, advanced threat detection, and next-generation firewalls) ▪ Restriction of local administrator privileges

Building a Resilient Environment

	Common Phase Activities	Example Controls
Escalate Privileges	▪ Remote misconfiguration or vulnerability exploitation ▪ Local misconfiguration or vulnerability exploitation ▪ Locate unsecured credentials ▪ Credential harvesting	▪ Host-based exploit prevention ▪ Internal vulnerability management ▪ Password vault secure credential storage ▪ Endpoint hardening procedures

Building a Resilient Environment

	Common Phase Activities	Example Controls
Internal Recon	▪ Port/service/vulnerability scanning ▪ Directory service queries ▪ Fileshare crawling	▪ Continuous anomaly detection ▪ Hardened directory services ▪ Network segmentation

Building a Resilient Environment

	Common Phase Activities	Example Controls
Lateral Movement	▪ Use of remote access protocols (e.g. WMI, PowerShell Remoting, PsExec) ▪ Abuse of remote administration services (RDP, SSH, etc.)	▪ Blocking host-to-host communication ▪ Network segmentation ▪ Multi-factor authentication

Building a Resilient Environment

	Common Phase Activities	Example Controls
Maintain Presence	▪ Command and control traffic ▪ VPN access via 2FA compromise ▪ Internet-facing web shells	▪ Network protection ▪ VPN activity monitoring ▪ Active threat hunting

Building a Resilient Environment

	Common Phase Activities	Example Controls
Complete Mission	▪ Encrypted split archives ▪ Data exfiltration ▪ Evidence wiping	▪ Continuous anomaly detection ▪ Active threat hunting ▪ Centralized logging ▪ Incident Response Plan

If the Worst Does Happen

Empathy

Collaboration

Communication

It’s the only way that we’ll successfully turn the tide.

Thank You

Questions?