IS YOUR ORGANIZATION READY FOR AUTOMATION?

January 9th, 2019
Is Your Organization Ready for Automation

Today’s web conference is generously sponsored by:

Rapid 7
https://www.rapid7.com/
Mikhael is Director of Information Security & Risk Management for Farmers Insurance. He is also an Advisor for Safe-T US Executive Advisory Committee. In the past decade he has taken on number of information security roles including engineering, teaching, writing, research and management. His sector experience includes insurance, defense, healthcare, nonprofit/education and technology/Internet, seeing first-hand the variance in information security culture and program maturity. Felker received his M.S. in information security policy and management from Carnegie Mellon University and B.S. in computer science from UCLA. He has over 50+ publications and has been a speaker for RSAC, CSA, ISSA, ISACA, ISC2 and OWASP events.
Michael Wylie, MBA, CISSP is the Director of Cybersecurity Services at Richey May Technology Solutions. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, cloud security, penetration tests, risk management, and training. He has developed and taught numerous courses for the U.S. Department of Defense, Moorpark College, California State Universities, and clients around the country. Michael holds credentials from certifying bodies such as ISC2, Cisco, VMware, GIAC, Dell, EC-Council, CompTIA, and more. During client security testing, Michael has identified and responsibly disclosed four zero-day vulnerabilities in major tax software in 2018.

Twitter: @TheMikeWylie
Is Your Organization Ready for Automation

Speaker

Jason Winder, Managing Partner, Aerstone Labs

Jason Winder has more than 20 years of experience in the information security field. He founded Aerstone in 2003, a boutique cybersecurity consultancy and service-disabled veteran-owned small business that is one of just five NSA-certified vulnerability assessors in the world. Aerstone's customers include some of the country's largest organizations and institutions in the federal, military, commercial, and intelligence sectors. Jason has an undergraduate degree in Economics from Drew University, and holds dual Master’s degrees from the Katz Graduate School of Business at the University of Pittsburgh, in Business Administration and International Business. His private interests include languages, golf, travel, writing, and cooking.
Scott has over 20 years of professional work experience in the IT and cybersecurity fields. He started his career as a network and systems engineer in the midst of the Silicon Valley dot com boom of the 90's. In 2001, Scott moved into an information assurance role supporting the Department of Defense, which kick started his career as a cybersecurity professional. Scott has worked for the DoD, state governments, large technology companies, mid-size manufacturing companies, and the spent significant time in the energy industry. Scott brings a unique mixture of hands-on experience in incident response, penetration testing, forensics, operations, architecture, engineering, and executive leadership as a former Chief Information Security Officer (CISO) to the Rapid7 Advisory team.
Mike Wylie, MBA, CISSP
Director, Cybersecurity Services
RICHEY MAY TECHNOLOGY SOLUTIONS

Additional
- GPEN
- CEH
- CEI
- CCNA CyberOps
- Pentest+

Certifications
- CCNA R&S
- Project+
- Security+
- CHPA
- VCP-DCA

Michael Wylie
@TheMikeWylie
www.RicheyMayTech.com
Michael@RicheyMay.com
Richey May Technology Solutions is a results-driven consulting firm offering the full spectrum of technology solutions for your business. Led by technology experts with decades of cumulative experience in executive IT roles, our team is able to bring you pragmatic, real-world solutions that deliver value to your business.
Critical Stats

➢ Average user receives 16 malicious emails/month (Symantec ISTR, 2018)

➢ 55% of enterprises trigger >10k alerts/day (RSA Survey, 2018)

➢ Average dwell time increases YOY - 101 days (Mandiant M-Trends, 2017)

➢ 0% unemployment rate in Cybersecurity (Forbes, 2018)

➢ By 2020, 15% of orgs with >4 security pros will adopt SOAR. Current adoption rate is <1% (Gartner, 2017)
Challenges

➢ Alert Overload
   ❑ False positives resulting in ignored alerts
   ❑ Difficult to distinguish normal events from attacks
   ❑ No one can act on 10k daily alerts

➢ Limited Resources & Shortage of Staff
   ❑ Staff’s time need to be optimized
   ❑ Global shortage of security pros

➢ Disperse Information
   ❑ Intel comes from numerous sources (ARIN, WHOIS, DNS Lookup, Logs, Threat Feeds, & Reputation Lookup)

➢ Manual Process

Alert ➔ Review ➔ Intel ➔ Intel ➔ Correlate Findings ➔ Conclusion ➔ Action
Before you start to SOAR:

- Map out processes
- Pick key processes to automate
- Enrich data to make better decisions
- Create high fidelity alerts
- Automate tangible information to act upon
Case Study

- University in California
- 6-7 IT staff with multiple hats (9am-5pm)
- Some experience in security - no dedicated FTE
- 2+ hours a day reviewing logs
- Primary attack vector = Phishing
- Hundreds of daily AV, SPAM, Firewall, etc.
- Major breach within the last 18 months
- Hired outsourced SOC & bought a bunch of tools
- Spinning wheels for over a year
Enrich, Automate, & Act

➢ Enrich data
  ❑ GeoIP
  ❑ WHOIS
  ❑ Alexa top 1M
  ❑ Fuzzy domains

➢ High fidelity alerts
  ❑ IP addresses originating from:
    ✓ Russia, North Korea, Iran, & China
  ❑ Domains registered <72 hours ago
  ❑ Exclude top 1M
  ❑ Domains like example.com

➢ Take confident action
  ❑ RIR lookup
  ❑ WHOIS lookup
  ❑ Domain registration date
  ❑ Firewall logs
  ❑ EDR logs

![Graph showing DNS alerts and excluded domains over time]
Enrich, Automate, & Act

➢ Enrich data
  ❑ Single Folder Object Auditing (a.k.a. HoneyFile)
  ❑ Detect randomness using NLP freq.py (Mark Baggett)

➢ High fidelity alerts
  ❑ Alert on read/write/modify of “HoneyFiles”
  ❑ Detect rename randomness using freq.py

➢ Take confident actions
  ❑ Isolate system
  ❑ Block action
Enrich, Automate, & Act

➢ Enrich data
  □ Create fake user profiles (a.k.a HoneyUser)
  □ Failed/Success logging for “HoneyUser”

➢ High fidelity alerts
  □ Any login attempt with “HoneyUser”

➢ Take confident action
  □ Reverse recon of attacker
  □ Collect information about attack attempts
  □ Block IP
QUESTIONS?
IdAM Automation

A core building block of enterprise security
About Jason Winder

➢ Specializes in large-scale enterprise identity and access management (IdAM) solutions.

➢ Founding Partner and IdAM Practice Lead of Aerstone, a boutique cybersecurity consulting company.

➢ Spent the last 20 years working complex IdAM efforts across the US Military, Federal Government, US Intelligence Community, and Private industry.

➢ Currently leading IdAM architecture and build-out for NATO’s new billion-dollar IT Modernization effort.
Scoping the Problem

➢ What is IdAM?
  ❑ Identity and access management (ID, AuthN, AuthZ)
  ❑ Defines and controls system access
  ❑ Touches at least five of the CIS-20 controls

➢ Why is IdAM important?
  ❑ Can’t have confidentiality without knowing who’s who
  ❑ Can’t have integrity without knowing what’s what
  ❑ Can’t have availability without managing access

➢ What does IdAM look like in most shops?
  ❑ Byzantine scripts
  ❑ Home-grown applications
  ❑ Poorly-integrated COTS software
Core IdAM Components

➢ HR System
➢ User Directory Platform
➢ Application Directory Platform
➢ Enterprise PKI Solution
➢ Metadirectory Synchronization
➢ Single-Sign On
➢ Multifactor Authentication
➢ Privileged Access Management (PAM)
➢ Cloud Access Security Broker (CASB)
➢ IdAM Governance Solution
The Automation Challenge

➢ Define Requirements
  ❑ Business Rules
  ❑ Users & Use Cases
  ❑ Enterprises Systems

➢ Evaluate Options
  ❑ On Premises Software
  ❑ Cloud-Based Services

➢ Implement Solution
  ❑ Gradual Cutover
  ❑ Monitor Progress
  ❑ Disruption is Inevitable!
Key Success Factors

➢ Spend the up-front time on business rules
➢ Avoid home-grown code wherever possible
➢ Consider multi-level security requirements
➢ Resist the temptation to over-complicate
➢ Create an override mechanism
➢ Work to upgrade legacy systems
➢ Implement an SA&A Process:
  ❑ Draw security boundaries
  ❑ Categorize systems (FIPS-199)
  ❑ Select security controls
  ❑ Assess systems against controls
Aerstone is a service-disabled veteran-owned small business with offices in MD, VA, and CO.

We support the military, intelligence community, federal government, and private industry with highest level cybersecurity consulting services.

We are one of just five NSA-certified vulnerability assessors in the world, under the NSA CIRA program.

For more information on our capabilities and services, please visit www.aerstone.com, or contact info@aerstone.com.
Scott has over 20 years of professional work experience in the IT and cybersecurity fields. He started his career as a network and systems engineer in the midst of the Silicon Valley dot com boom of the 90's. In 2001, Scott moved into an information assurance role supporting the Department of Defense, which kick started his career as a cybersecurity professional. Scott has worked for the DoD, state governments, large technology companies, mid-size manufacturing companies, and the spent significant time in the energy industry. Scott brings a unique mixture of hands-on experience in incident response, penetration testing, forensics, operations, architecture, engineering, and executive leadership as a former Chief Information Security Officer (CISO) to the Rapid7 Advisory team.
The Need for Security Orchestration & Automation
The global cybersecurity workforce will be short by around 1.8M people by 2022, representing a rise of around 20 percent since 2015, according to a new report by Frost & Sullivan.
UNINTEGRATED TOOLS AND SYSTEMS

The average enterprise uses 75 security products to secure their network.
TOO MANY ALERTS

Thousands competing for the security team’s attention per day.
Time and Resources Are Not Unlimited
REPETITIVE, MANUAL PROCESSES
STEP 1:

Define your organization's pain points
• Does your security team get too many alerts to handle effectively and in a timely fashion?

• Is your team suffering from symptoms of burnout?

• Do you have trouble hiring and/or retaining security talent?

• Does your team spend an inordinate amount of time gathering and analyzing information?

• Is your mean time to respond to a threat getting worse?
STEP 2:
Define your most common use cases
Commonly Automated Use Cases

Increase efficiency across your organization

- Automated Patching
- Malware Investigation & Containment
- Provisioning & Deprovisioning
- Privilege Escalation Investigations
- Email Phishing Investigations
- Threat Hunting
- Security Alert Data Enrichment
- Much More
STEP 3:
Understand your people, processes, and tools
LEARN YOUR PEOPLE
VALIDATE YOUR PROCESS

Request for access?

- IT validation with managers / system owners
- Manually creating accounts

Access Granted
UNDERSTAND YOUR TECHNOLOGY

[Diagram of an app management interface with the word 'APP' repeated across different sections]

RAPID7

ISSA
Information Systems Security Association International
QUESTIONS?