solutions

Automated Continuous Monitoring (ACM), and Ask Cyber

Jason B. Carrier, SDA Solutions, LLC

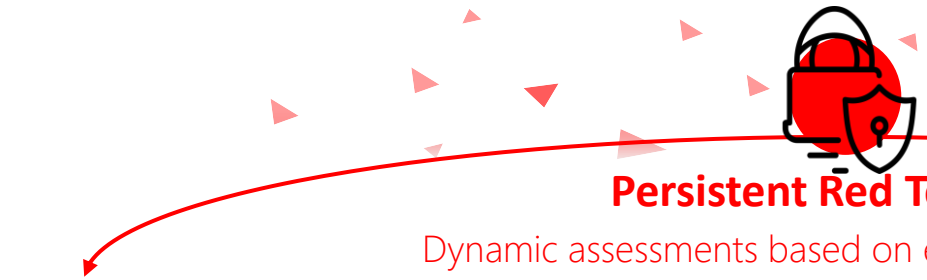
Agenda

- Introducing Automated Continuous Monitoring (ACM)
- Initiating the ACM Process
- Identifying and Integrating the Right Tools
- Counting is King
- Exploit validation
- Questions

Intro to Automated Continuous Monitoring

- Risk Management Framework (RMF) establishes need to monitor security and privacy control implementation and effectiveness
- EO 14028 and National Security Memo (NSM)-8 codify the need for ACM as a critical component of Zero Trust Architecture (ZTA)
  - *Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment.*
- Memorandum for Senior Pentagon Leadership Defense Agency and DoD Field Activity Directors 0222
  - Continuous ATO (C-ATO) needed to promote innovation and outpace evolving cyber threats
  - Ongoing visibility is key to enabling active cyber defense
  - AOs must be able to centrally monitor cumulative sets of controls across their AOR to make risk-informed decisions (e.g., dashboards)
  - Active penetration testing

ACM Is More Than Periodic Scanning



Persistent Red Teaming

Dynamic assessments based on evolving threat vectors

Threat Intelligence

Actionable data on evolving TTPs and vulnerabilities

Automated ConMon

Compliance

Achieving and sustaining ATO for networks, systems, applications, databases, and peripherals

Threat modelling

Appling threat intelligence to understand exposure

Network Operations

Monitoring, managing, and responding to performance issues

Security Operations

Monitoring, managing, and responding to security issues

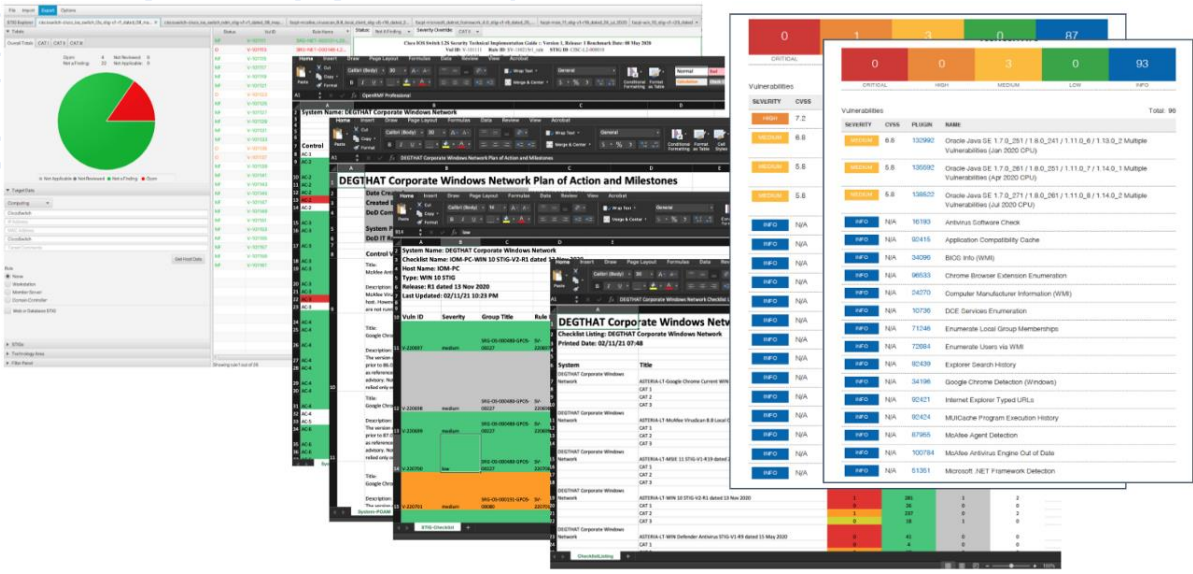
Initiating the ACM Process

- RMF Starts During Development
  - Understanding High Value Assets (HVAs)
  - Design Controls to Protect HVAs
  - Static Code Analysis
  - Implementation and Training Guides
- ConMon Starts After Deployment
- Start With What You Have
  - Plan for Gaps You Identify
- Control-to-Technology Mapping
  - CSSP Tools (SIEM, SOAR, GRC, and Scanners)
  - Firewalls, IDS/IPS, and CND Tools
  - Automate Monitoring and Alerts

Tools	# of RMF Controls	CyberSecurity Framework (Identify, Protect, Detect, Respond ,Recover)
C2C (Forescout)	150	Identify, Detect
RedSeal	48	Identify, Detect
ACAS	49	Identify, Detect
Illusive	22	Identify, Detect, Respond, Recover
HBSS	76	Detect, Respond
AttackIQ	60	Identify
ExtraHop	190	Identify, Protect, Respond
Archer	5	Detect, Respond
Elastic SIEM	42	Identify, Protect, Detect, Respond
DoD PKI	31	Identify
Total	578	All

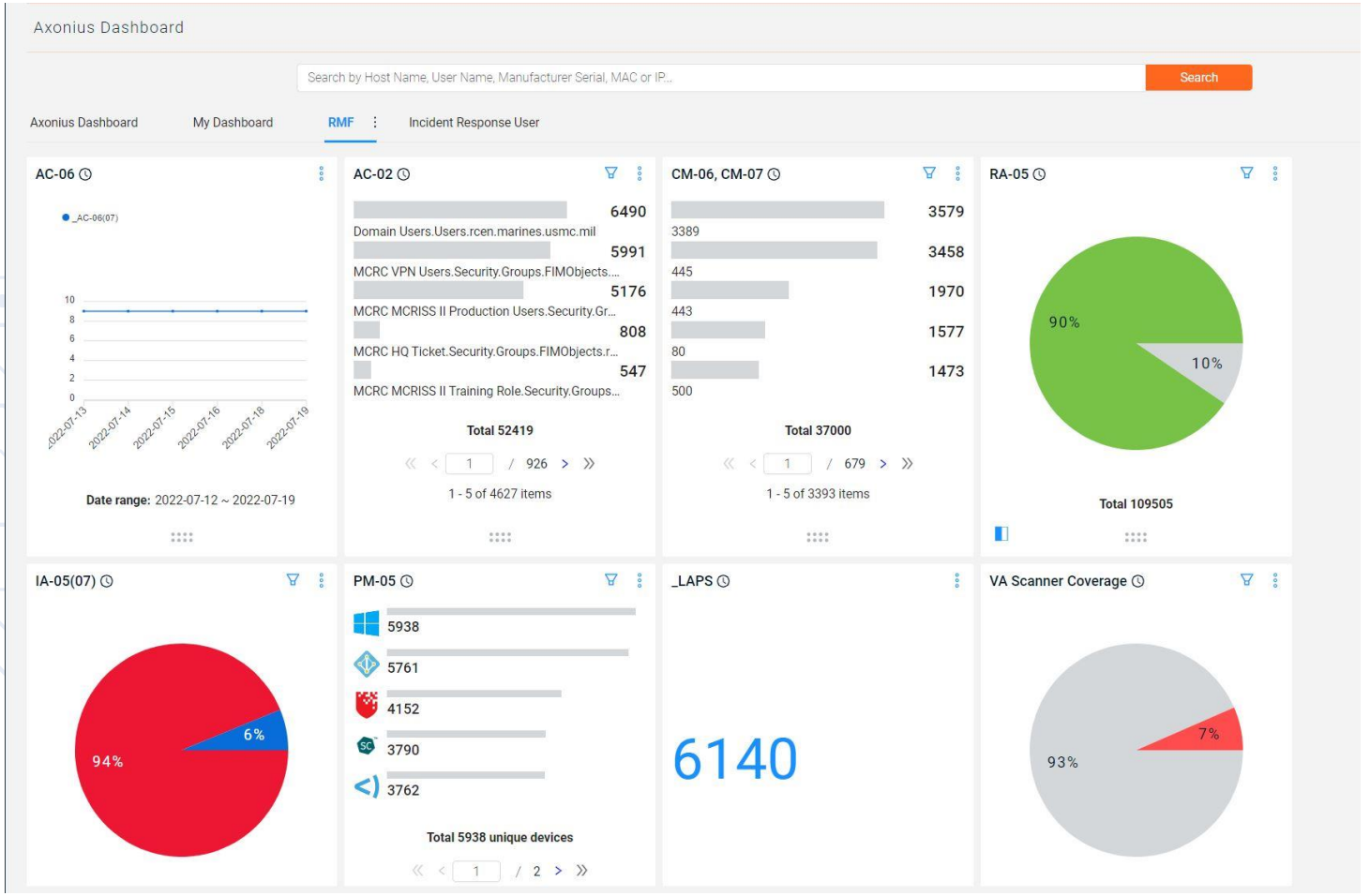
Identifying and Integrating the Right Tools

- Standard DoD Stack
  - ACAS, HBSS, ForeScout, Tanium
- STIG Checkers
  - Evaluate-STIG (JSON adapter)
- Security Incident and Event Management (SIEM)
  - Exabeam, Darktrace, Elastic, Splunk, Gravwell, etc
- Network Detection and Response (NDR)
  - ExtraHop, Vectra, Zeek, Bricada, etc
- Endpoint Detection and Response (EDR)
  - Windows Defender, HBSS
- Other



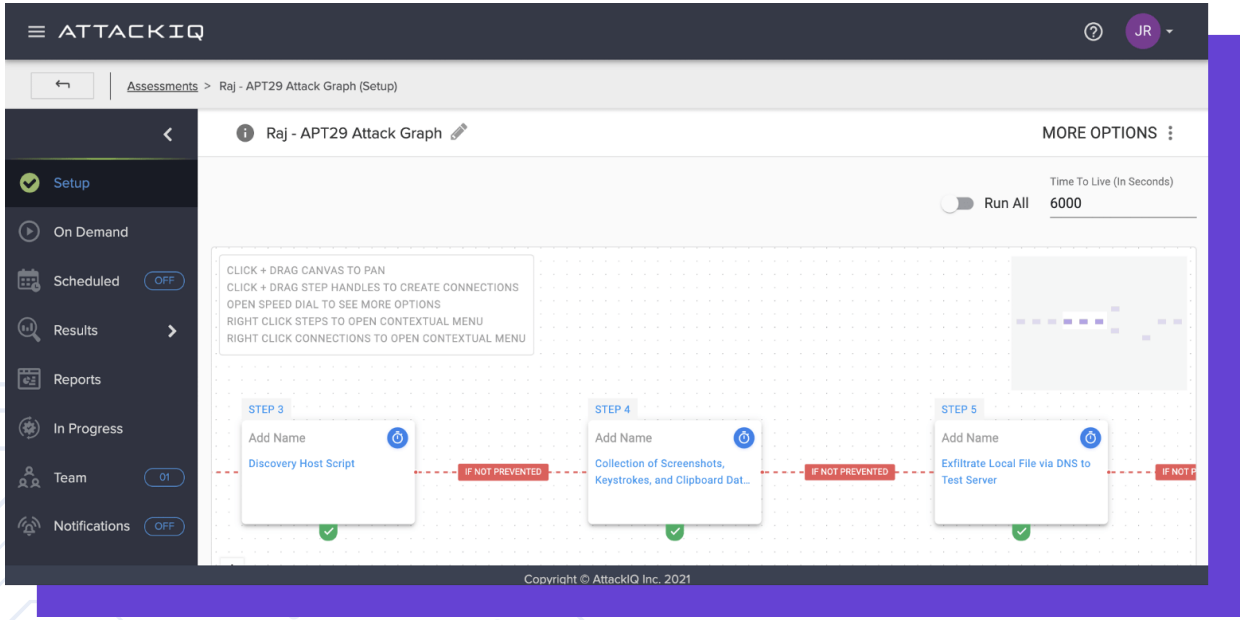
Counting is King

- Data Aggregator & Normalization
  - Axonius
  - Data correlation and Deduplication
  - Limited SOAR Function
  - 800+ Connectors
  - Shadow IT
  - Baseline deviations
  - Both technical and non-technical controls
- eGRCs
  - eMASS, Archer, Logigate, ServiceNow, Pathlock, MetricStream



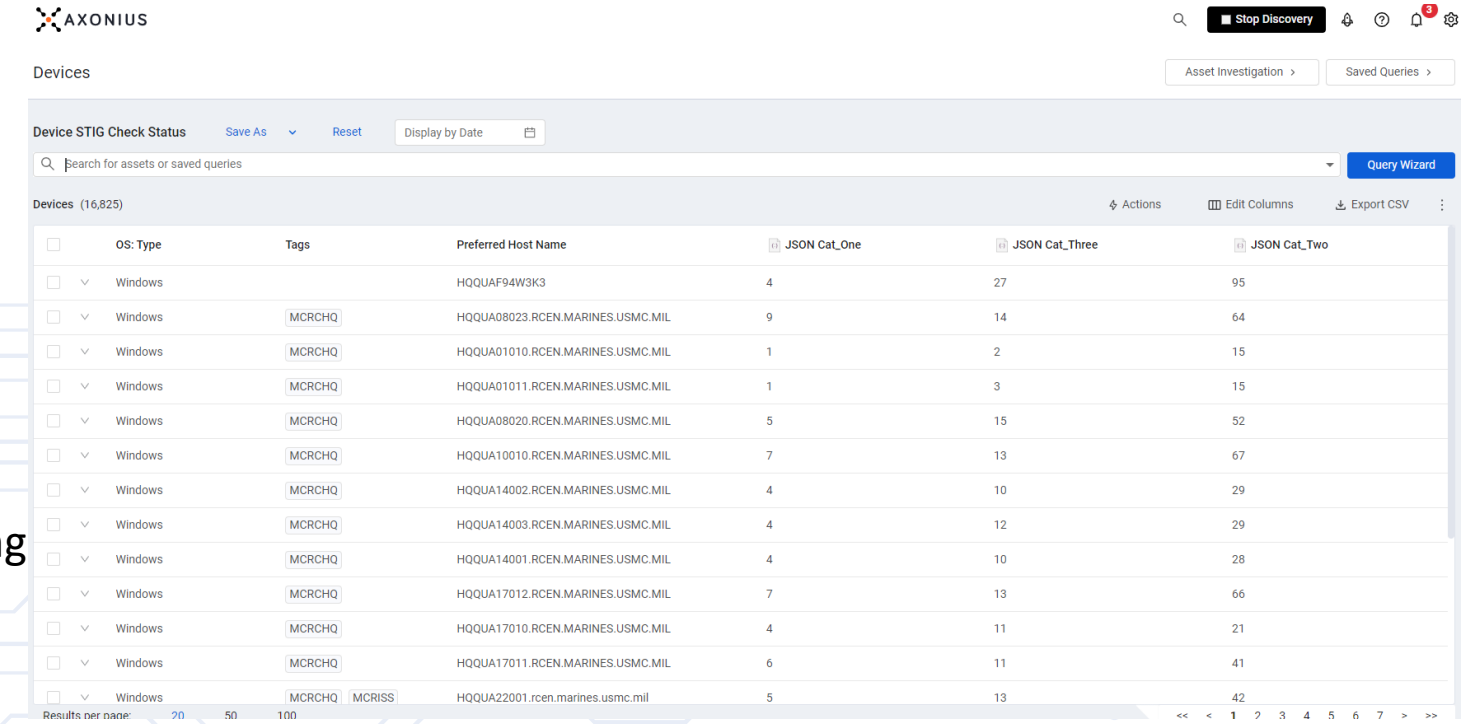
Exploit validation

- Breach and Attack Simulator (BAS)
  - Attack IQ (August 1st, 2023), others
- Not vulnerability scanning
- Testing CVEs against current defenses
- Measures response for Defense in depth tools
  - Measures tool efficacy
  - Show residual risk
  - Allows to capitalize on security investments
- Test named exploits and APT actors based on threat intelligence.



Additional Use Cases

- Threat Hunting
  - Aggressive Nomad
  - Public Facing Exploits
  - PowerShell
  - Python
- Automated CCRI
  - ACAS scans, STIG Checks, Scoring
- Comply to Connect
  - Automated Patching
  - Isolation of host
  - Self Healing assets



- Automated vulnerability risk assessment and scoring

Questions?

Jason B. Carrier, SDA Solutions, LLC

jason.carrier@sdasolution.com