D3FC0N

Down the Rabbit Hole: 10 Lessons Learned from a Year in the Trenches

Andrew Costis

>> whois <<

- Andrew Costis / “AC”
- Senior Cyber Threat Consultant ATTACKIQ®
- 20+ Years industry experience
  - 5+ years threat research, malware RE, DFIR


@0x4143


/andrewcostis/


/0x4143

>> Motivation <<

- To share some practical tips, tricks and advice based on my own journey and experiences
- Applicable to both technical and non-technical peers
- Applicable to:
  - Breach and Attack Simulation (BAS)
  - Threat/Adversary emulation
  - Red/Blue/Purple teaming
  - Security Control Validation
  - Security Optimization
  - Threat-Informed Defense
  - DIY/in-house/BYOTTPs©
  - Related new/upcoming/trending buzz-words/acronyms/terms

>> Misc <<

- Top 10 Lessons are in no particular order
- Assumed *basic conceptual* understanding of key terms
- Random British pictures added for good measure

>> 1: Understand the Environment <<

- Inventory, map, document as much as possible
- Business structure, departments, regions, business units
- Network topology
- Data flow, patterns, users
- Cloud, on-prem assets
- Crown jewel applications
- Security controls
- Eases pain when scaling out, planning assessments, triaging and remediating

>> 2: Understand the Security Objectives <<

- Regulatory / compliance
- Threat of the week
- Targeted attacks, TA specific
- OS specific
- Insider threats
- SOC augmentation
- Cloud threats
- Security control validation
- Warning: goal posts likely to change!

>> 3: Stakeholder Support <<

- Critical for long term success and adoption
- Gets on everybody's radar
- Helps in staying aligned
- Break through barriers
- People come and go (churn)
- Meet regularly to:
  - Prioritize work
  - Identify challenges
  - Scope creep
  - Discuss progress
  - Set action items

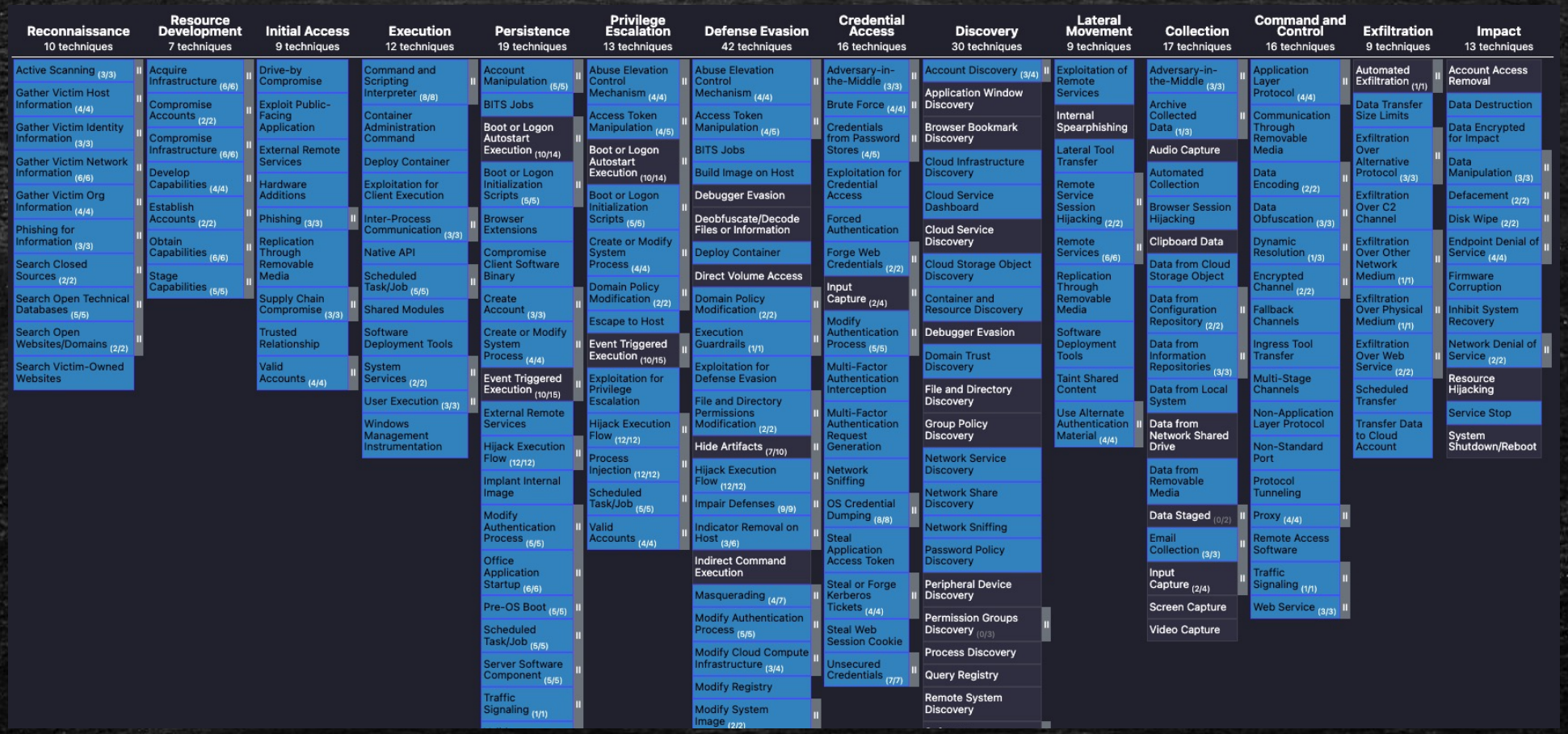
>> 4: Information Sharing & Collaboration <<

- Decide and agree on a central place to store your work
  - E.g. Teams, GitHub, Jira, Vectr.io, SharePoint, Excel
- Decide on access control early on (due to sensitivity)
- Junior (green) audience
- Plan for scale/growth in mind
- Be as granular as possible
- Likely to include:
  - Security control configuration
  - Assessment/test specific configuration
  - Detection info / log, alert output
  - Mitigation/remediation notes
  - TTPs tested

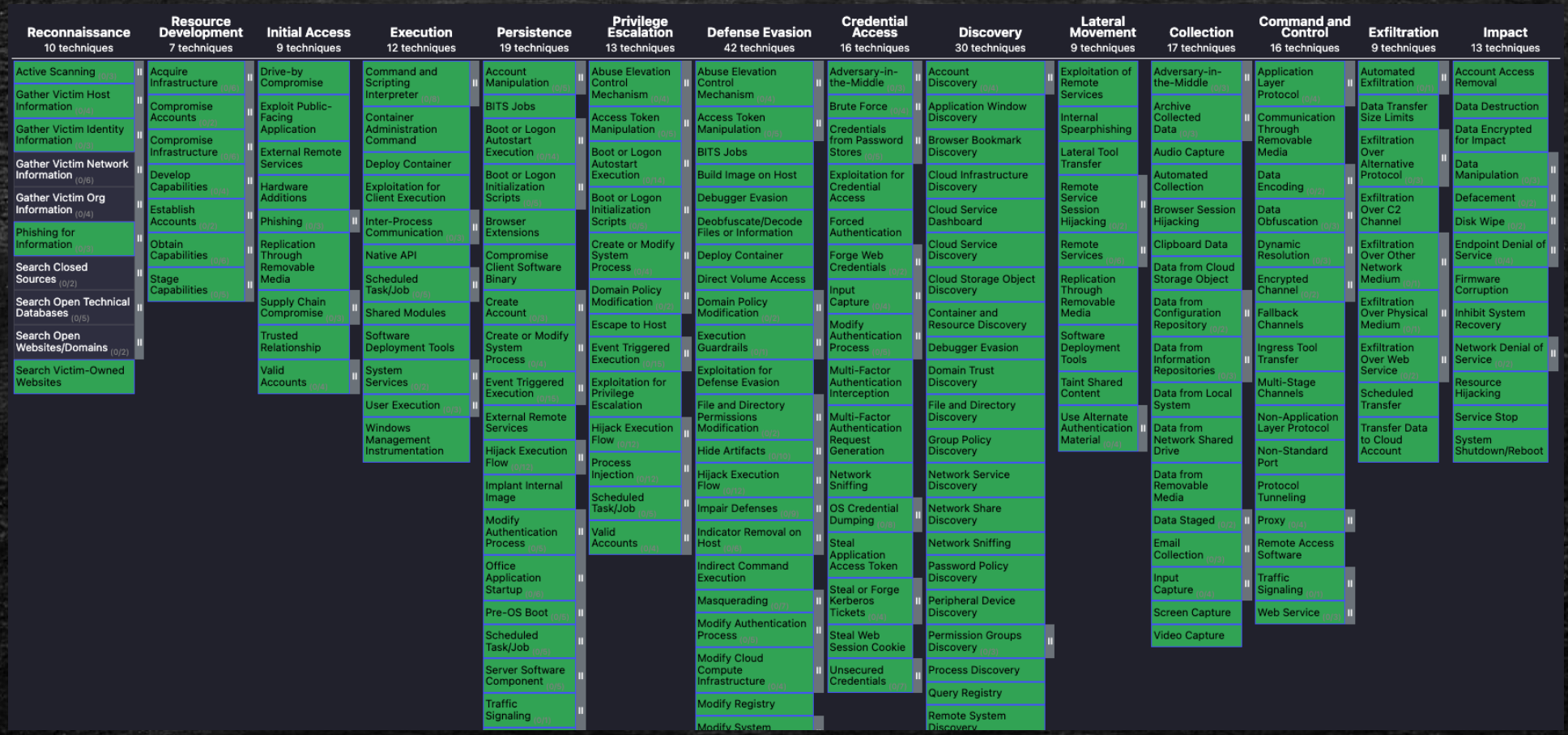
>> 5: Detection vs Prevention <<

- Prevention is often the preferred choice
- Some TTPs may be too complex to prevent
- Detection will likely be a more realistic near-term goal
- Detection provides invaluable and much needed visibility
- Not easy to patch/mitigate/remediate legacy systems
- Defense in depth approach

>> Techniques with Mitigations <<

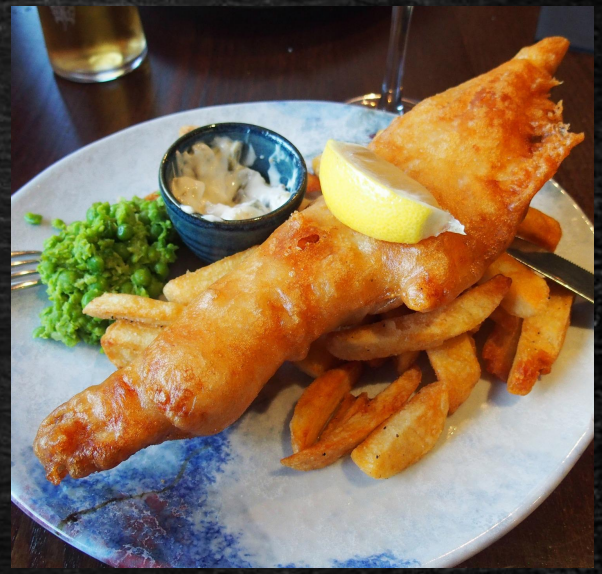


>> Techniques with Data Sources <<



>> 6: Direct vs Indirect Findings <<

- Direct Finding:
  - **Event Triggered Execution: WMI Event Subscription (T1546.003)** using .mof files is prevented and/or detected by 'X' security control
- Indirect Finding:
  - **Application Layer Protocols: Web Protocols (T1071.001)** using exfil of dummy data is detected, but detection took >4 hours for the alert to arrive, resulting in the SOC missing the alert
  - **Windows Management Instrumentation (T1047)** using *wmic process call create* isn't prevented and/or detected due to Endpoint sensor not checking in, not installed, or wrong policy applied, subsequently resulting in a test binary executable being able to launch
- Will likely observe indirect findings throughout
- Continuous automated testing at scale will bring both to the surface
- Key to improving overall security posture and maturity



>> 7: Start Small <<

- Requires careful planning and scoping
- Identify test hosts early on (dedicated or temp)
- Baseline where possible
- Test in production when confident
- Focus on a few TTPs, or a small section of an attack chain first, in order to test out your process and workflow
- Quality vs quantity
- The more you test, the more findings you will uncover
  - Not always a good thing…
- Network TTPs are a good place to start

>> 8: Purple Teaming <<

- Establish early on
- Regular meeting cadence critical to continuity
- Ability to obtain a range of input
  - Intelligence-led
- What's keeping them up at night?
- Designed to support & augment each other's workloads and priorities
- Narrative/story
  - Useful in supporting wider initiatives
  - Top ATT&CK Techniques – CTID project

>> 9: Automation <<

- If repeating a task more than once, automate where *feasible*
- Automate assessments
  - (integral to uncovering when drift occurs in the environment)
- Red team engagements >> adversary emulation
  - Procedural level details help
- Reporting
  - Assessments, weekly, monthly
- API integration with security controls
- CTI ingestion

>> 10: Slow and Steady Wins the Race <<

- Rome wasn't built in a day
- Touches on all aspects and layers of security
- Enjoy the journey
- Don't make assumptions
- Motivation and persistence required
- Get familiar with free resources:
  - /ox4143/adversaryemulation-gems

>> Thank You <<


@0x4143


/andrewcostis/


/0x4143