Project 6.2 - 24x7 SOC - Logging Standard Update

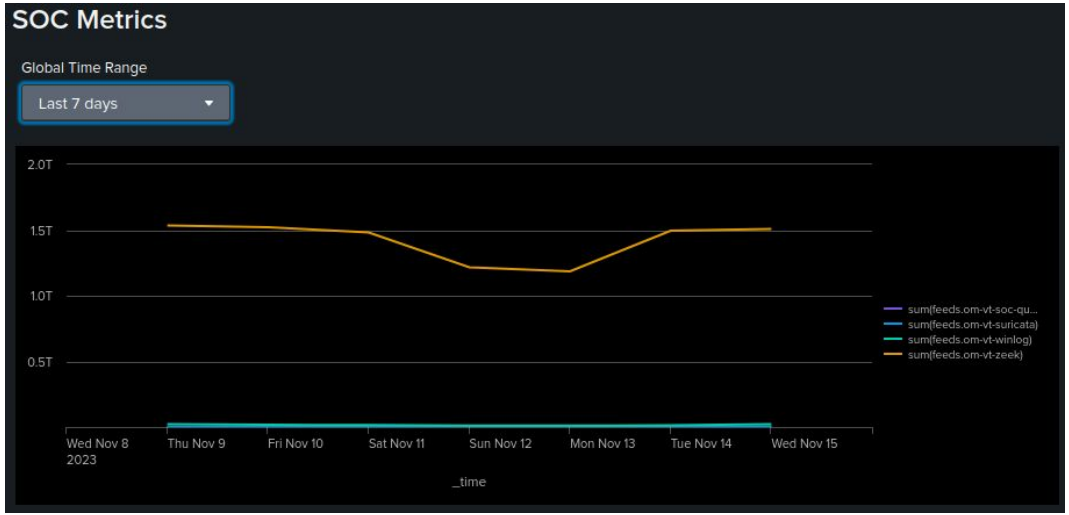
October 10, 2017

Crystal O'Graphie, Chemistry Department, Virginia Tech

VIRGINIA TECH™

OmniSOC Data

- VT data sent to OmniSOC
  - ~1.5 TB per day
- OmniSOC incidents opened since March 1
  - 29 Incidents opened
  - Daily communications back and forth with OmniSOC
- Currently working with OmniSOC to include MDE high severity alert data



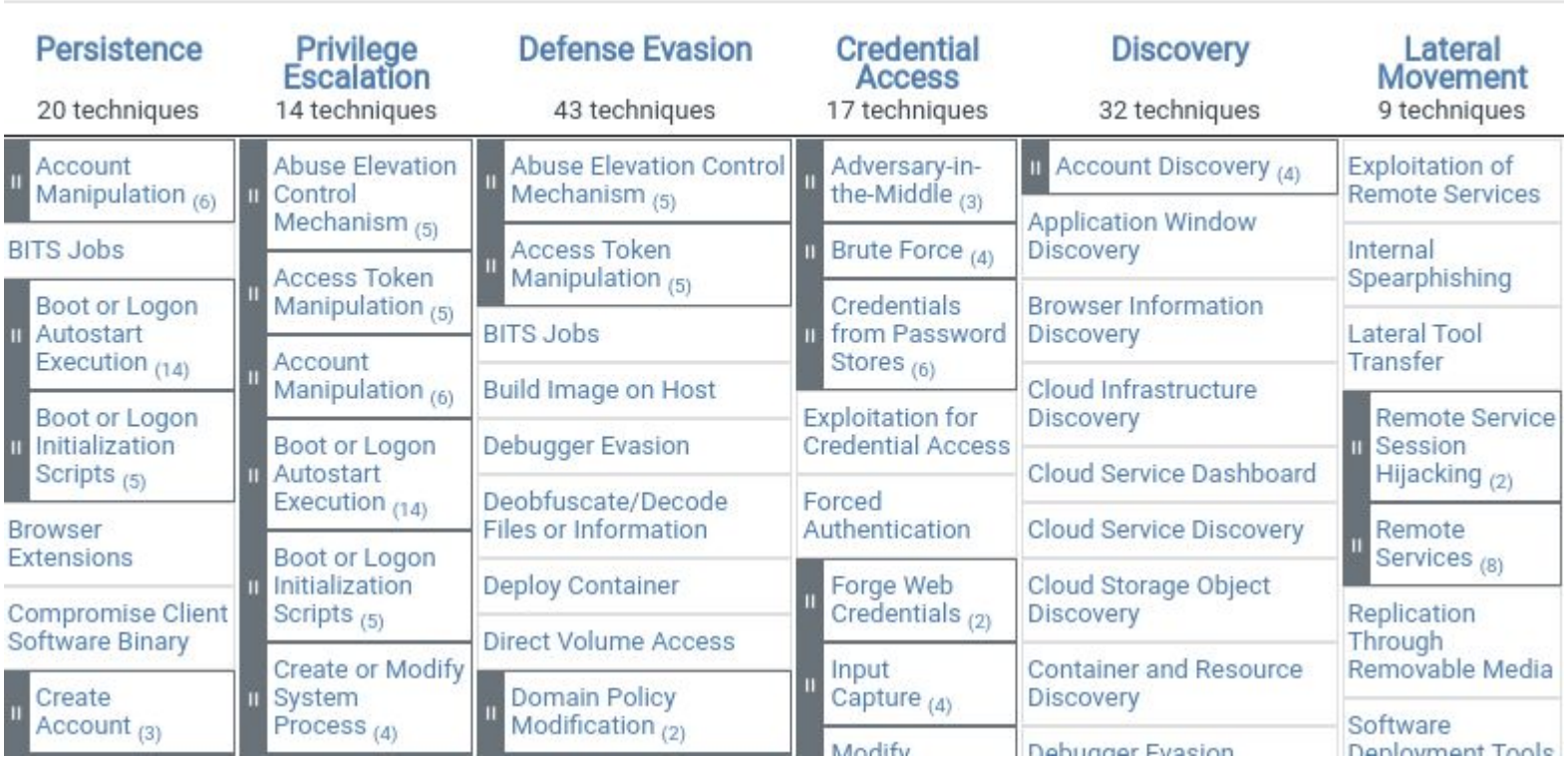
VIRGINIA TECH™

VT Logging Standard

- Policy 7010 - references the Minimum Security Standard
  - https://policies.vt.edu/assets/7010.pdf
- Minimum Security Standard - Defines sending logs to central logging service
  - https://it.vt.edu/content/dam/it_vt_edu/policies/Minimum-Security-Standards.pdf
- Standard for Information Technology Logging
  - https://it.vt.edu/content/dam/it_vt_edu/policies/Standard_for_Information_Technology_Logging.pdf
- Logging is implemented using Central Logging Service (with Splunk)
  - https://4help.vt.edu/sp?id=kb_article&sys_id=04014b751b9c7dd063110f66624bcb2d
- Sophos report states 82% of all incidents included disabling or wiping logs
  - https://news.sophos.com/en-us/2023/11/14/active-adversary-for-security-practitioners/

OmniSOC next steps

- OmniSOC is building out new set of detections currently based on Windows logging
- This is using the MITRE ATT&CK framework
  - MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
  - https://attack.mitre.org/
- This has the potential to be expanded Syslog based logging for Apple and Linux platforms
- To take advantage of these detections, you must be sending your logs to CLS



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques
Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services
BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing
Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer
Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)
Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media
Create Account (3)		Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	
		Direct Volume Access	Modify	Container and Resource Discovery	Software Deployment Tools
		Domain Policy Modification (2)		Debugger Evasion	

VIRGINIA TECH

Splunk Dashboards to share

- Working group has meet to define some dashboards we
- A beta version is under development
- We have done two Splunk trainings and videos are available
- Plan to have more of them as we proceed

Questions?