Purple Team Lifecycle

Overall
Status: **Completed**

PB1140 - Domain Password Spray

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- ⚪ Lifecycle Kickoff: 2/1/2021
- ⚪ Simulation Start: 2/3/2021
- ⚪ Simulation End: 2/6/2021
- ⚪ Configuration Identified: 11/29/2020
- ⚪ Change Management Referred: 2/6/2021
- ⚪ Configuration Deployed: TBD

Status Code Legend

🔴 Attack Simulation	🟡 System Configuration Change
🔵 Defense Simulation	⚪ Information

APT Lifecycle Ingest and Research	⚪ Lifecycle Type: **Attack Simulation** ⚪ Lifecycle Objective: **Alert**	⚪ Ingest Source: Atomic Purple Teaming ⚪ **Mitre T1110.003** https://attack.mitre.org/techniques/T1110/003
	⚪ Use domain password spray to check for common passwords. Identify this activity in logs.	

Attack methodology	🔴 Use DomainPasswordSpray.ps1 to spray the domain controller authentication process.
	`powershell -ep bypass`
	`Import-module .\DomainPasswordSpray.ps1`
	`Invoke-DomainPasswordSpray -Password Winter2020!`	

Defense methodology	🔵 Search within optics stack for evidence of execution of password spray. Select the logs-endpoint-winevent-security-* index Toggle the event. Action, event_status_value, and user_name fields as columns The hunt involves timeline analysis and inspection of log entries. Note event.code 4624 and 4625 and event_status_value "Account logon with misspelled or bad password"	
Lifecycle Adjustments	🟡 Additional changes to the optics stack were not necessary, however attention was made to event.code 4624 or 4625 while analyzing on a timegraph. Aggregation can be used for threshold alerting.	
Change Management	🟡 Deploy threshold alert for event.code 4624 /w event_status_value "User logon with misspelled or bad password" 🟡 Affected Users: Password Spray compromised account of **Luis.Graves** 🟡 Rollback: Remove alert of aggregate threshold	
Lessons Learned	⚪ Strong password policies can limit the effects of a password spray.	