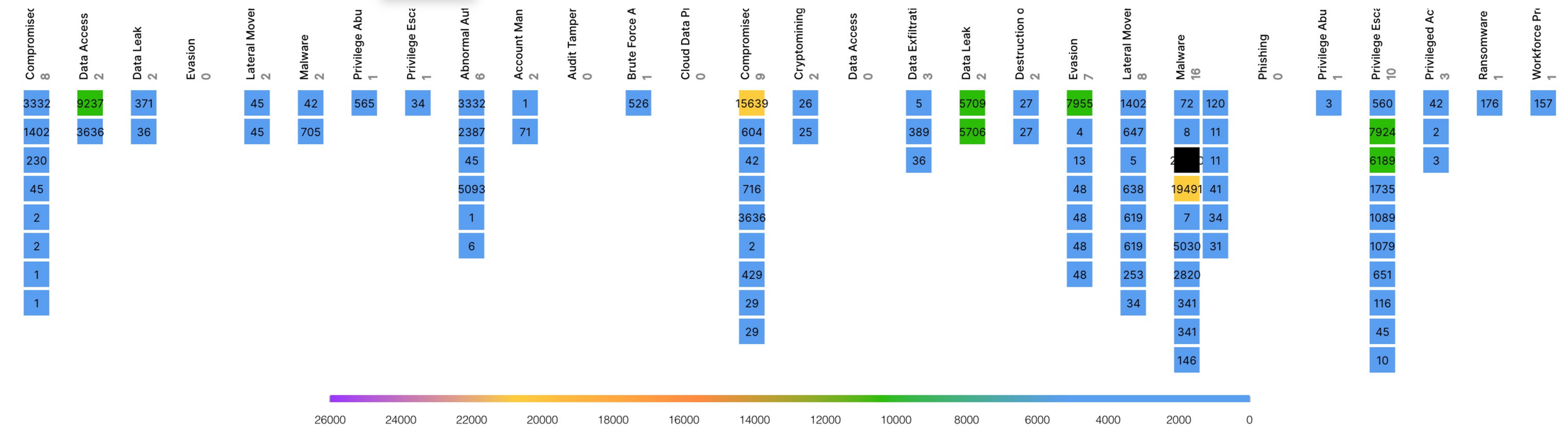
Exabeam - Mitre Coverage Threat Hunt

Edit

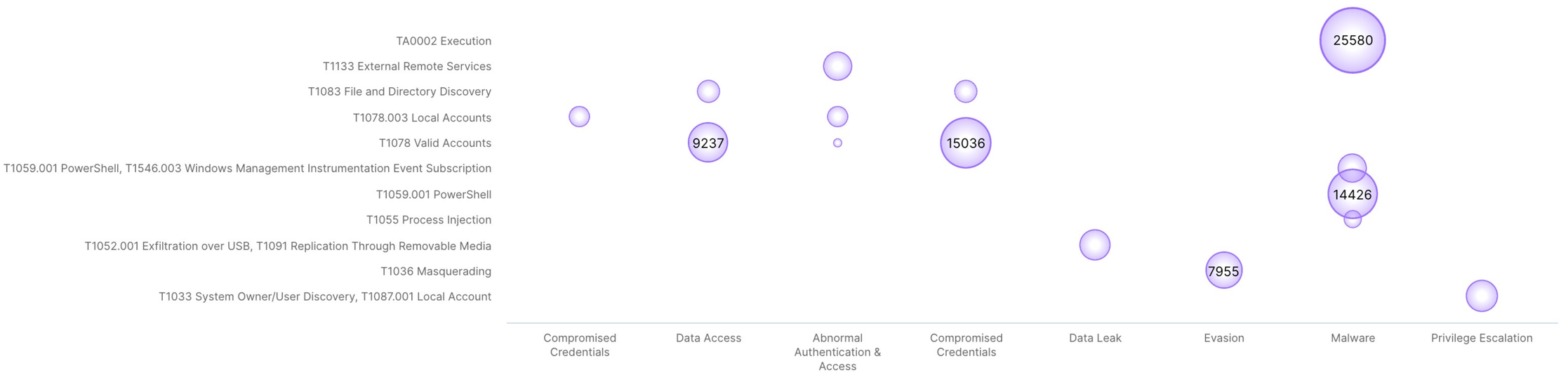
Total Rule Triggers Last Day

ASSET	USER
159	40,305

Mitre Use Case Coverage



MITRE Technique to Exabeam Use Cases



Last 10 Use Cases - MITRE Threat Hunt

Account Manipulation	T1098	AM-OG-F	1
Evasion	T1070.001	EventLog-Tamper	1
Evasion	T1070	Unauthorized-MBR-Mods	1
Malware	Change Default File Association	FileType-Association-Change	1
Malware	T1059.001	EPA-PU-PS-A	1
Compromised Credentials	Valid Accounts	VPN27	1
Compromised Credentials	File and Directory Discovery	FA-GD-F	1
Account Manipulation	T1484	DS-USH-F	1
Evasion	Indicator Removal on Host	Unauthorized-MBR-Mods	1
Malware	TA0002	EPA-UP-Commands-F	1

EVENT MITRE LABELS
T1484

Bottom 20 Triggers - MITRE Asset Hunt

Compromised Credentials	Abnormal asset running network sniffing tool	1
Malware	First execution of csc.exe to compile a malicious code on this asset.	1
Lateral Movement	Remote Powershell session was detected by monitoring for wsmprovhost as a parent or child process on this asset.	1
Malware	Abnormal execution of csc.exe to compile a malicious code	2
Evasion	A Windows program executable was started in a suspicious folder on this asset.	3
Privilege Escalation	The permissions of a file or folder were modified on this asset.	3
Malware	Windows shell has spawned a suspicious process on this asset	4
Compromised Credentials	First web activity event on asset	4
Malware	Svchost.exe has launched without any command line arguments on this asset	7
Malware	PowerShell was spawned via WMI on this asset.	41
	Non-Interactive Powershell activity was found on this	

Bottom 20 Triggers - MITRE User Hunt

Data Access	First file server access for group	1
Abnormal Authentication & Access	First local logon to asset	1
Account Manipulation	MMC (Microsoft Management Console) started a Windows command line executable.	1
Compromised Credentials	First file server access for group	1
Abnormal Authentication & Access	Abnormal number of logon assets (M)	1
Compromised Credentials	Abnormal user has run a network sniffing tool	1
Data Leak	First print activity from printer for user	1
Evasion	Bcdedit.exe has signs of malicious unauthorized usage.	1
Account Manipulation	First directory service activity on source host for user	1
Compromised Credentials	First Kerberos logon for abnormal pre-authentication type for the user	1
Account Manipulation	Abnormal group management activity from asset for user	1
Privilege Abuse	Abnormal group management activity from asset for user	1
Malware	Suspicious 'schtask' creation, possible attack tool usage	1