06-21-19

Using Queries as Building Blocks to Support Your Security Framework

Jon Nelson

Carbon Black.

Introduction

Jon Nelson

Carbon Black

Taught for the government

Pa. State Police, retired

Using osquery extensively since our adoption into Live Query

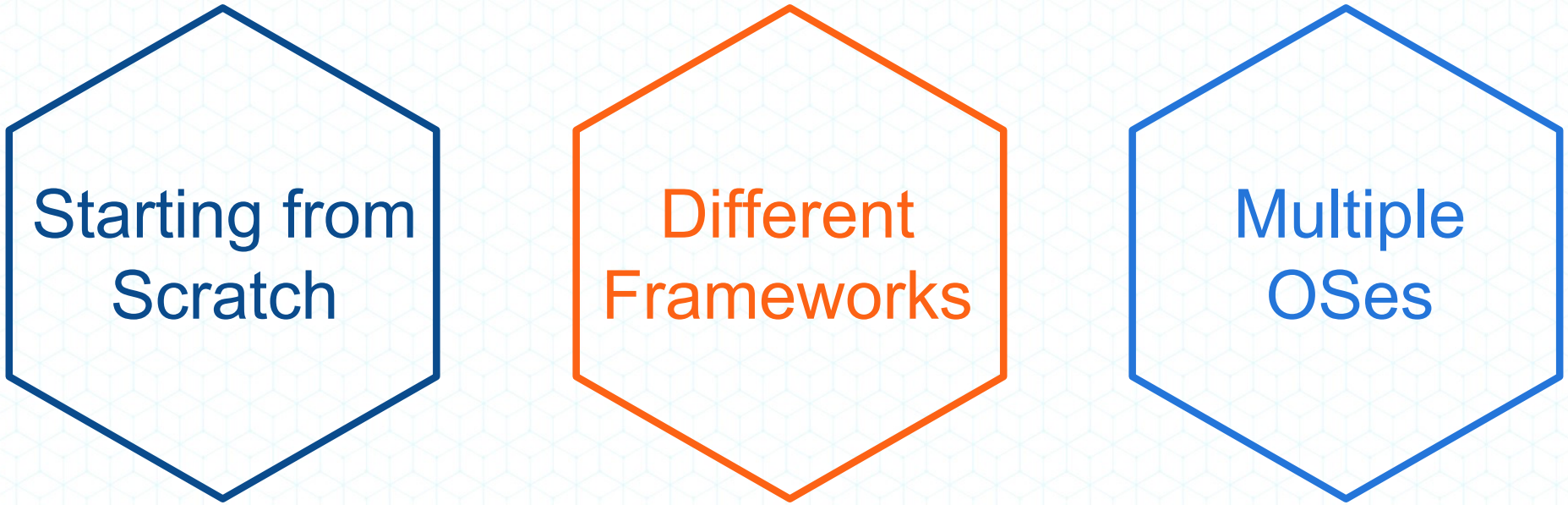
Carbon Black.

About last night...

```
osquery> select name,serverity from hangover;
+--------------------------+-------------+
| name                     | serverity   |
+--------------------------+-------------+
| Jon Nelson               | 6.42        |
+--------------------------+-------------+
```


Carbon Black.

Disabled services query - variables



2400+ data attributes

Carbon Black.

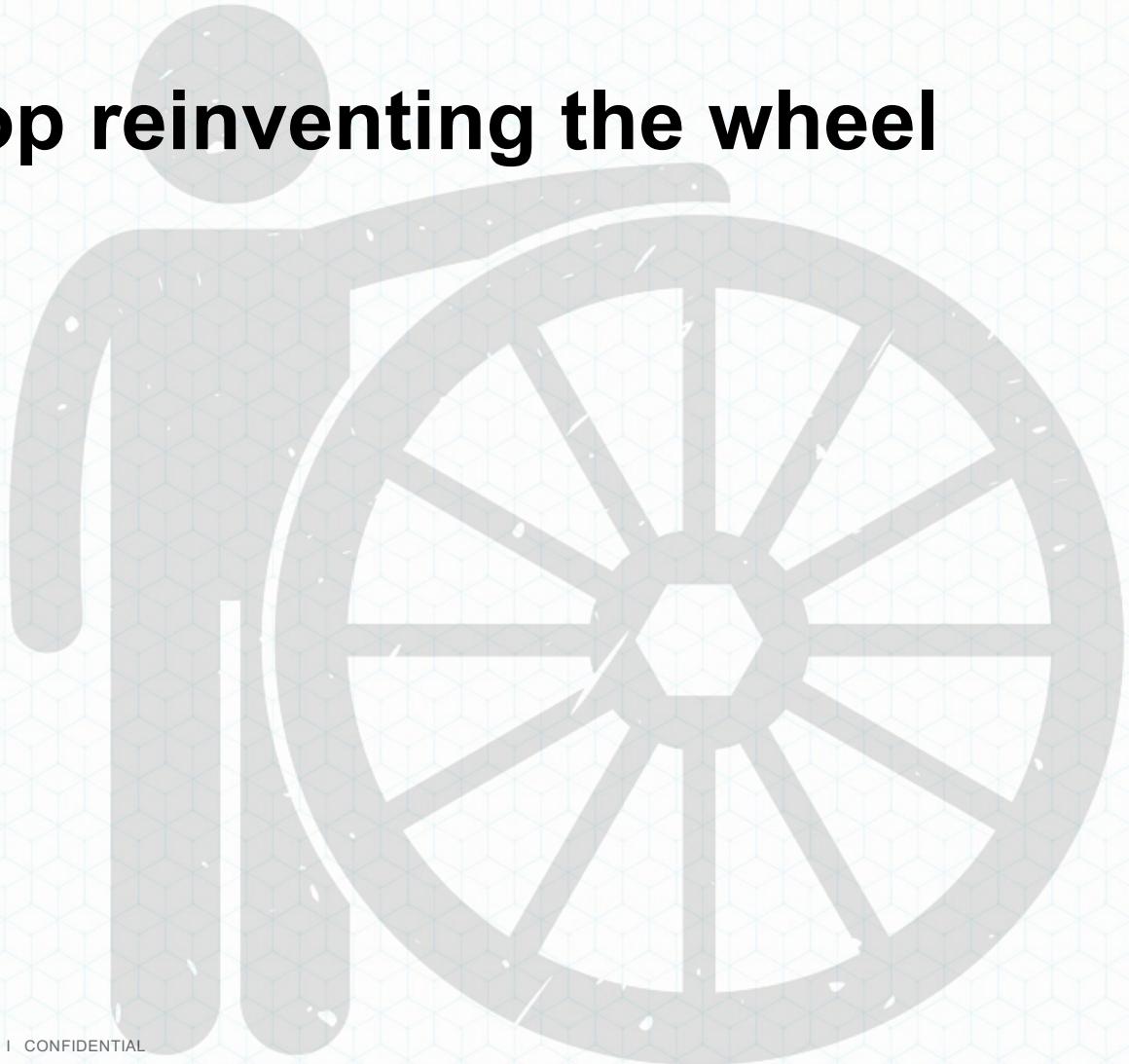
Querying based on business need

Security

IT Ops

Vulnerability Mgt

Let’s stop reinventing the wheel



Carbon Black.

Query Matrix

MITRE Enterprise ATT&CK™ Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery		Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain		Pass the Ticket	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	Security Software Discovery	Replication Through Removable Media	Trap	Screen Capture	Exfiltration Over Other Network Medium	
Dylib Hijacking		Space after Filename	Bash History			Source	Data Staged		Communication Through Removable Media
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Launchctl	Input Capture	Exfiltration Over Alternative Protocol	
AppInit DLLs		HISTCONTROL			Remote Desktop Protocol	Space after Filename	Data from Network Shared Drive		Multilayer Encryption
Web Shell		Hidden Users	Account Manipulation	System Owner/User Discovery	Pass the Hash	Execution through Module Load		Data Transfer Size Limits	Standard Application Layer Protocol
Service Registry Permissions Weakness		Clear Command History	Replication Through Removable Media		Exploitation of Vulnerability		Data from Local System	Data Compressed	
Scheduled Task		Gatekeeper Bypass		System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Data from Removable Media		Commonly Used Port
New Service		Hidden Window	Input Capture		Logon Scripts	InstallUtil			Standard Cryptographic Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Network Sniffing	Application Window Discovery	Remote Services	Regsvr32			
Path Interception			Credential Dumping		Application Deployment Software	Execution through API			Custom Cryptographic Protocol
Accessibility Features		Trusted Developer Utilities	Brute Force	Network Service Scanning		PowerShell			Data Obfuscation
Port Monitors		Regsvcs/Regasm	Credentials in Files	Query Registry	Remote File Copy	Rundll32			Custom Command and Control Protocol
Screensaver	Exploitation of Vulnerability			Remote System Discovery	Taint Shared Content	Scripting			
LSASS Driver	Extra Window Memory Injection			Permission Groups Discovery		Graphical User Interface			Connection Proxy
Browser Extensions	Access Token Manipulation			Process Discovery		Command-Line Interface			Uncommonly Used Port
Local Job Scheduling	Bypass User Account Control			System Service Discovery		Scheduled Task			Multiband Communication
Re-opened Applications	Process Injection					Windows Management Instrumentation			Fallback Channels
Rc.common	SID-History Injection	Component Object Model Hijacking				Trusted Developer Utilities			
Login Item	Sudo	InstallUtil				Service Execution			
LC_LOAD_DYLIB Addition	Setuid and Setgid	Regsvr32							
Launch Agent		Code Signing							
Hidden Files and Directories		Modify Registry							
.bash_profile and .bashrc		Component Firmware							
Trap		Redundant Access							
Launchctl		File Deletion							
Office Application Startup		Timestomp							
Create Account		NTFS Extended Attributes							
External Remote Services		Process Hollowing							
Authentication Package		Disabling Security Tools							
Netsh Helper DLL		Rundll32							
Component Object Model Hijacking		DLL Side-Loading							
Redundant Access		Indicator Removal on Host							
Security Support Provider		Indicator Removal from Tools							
Windows Management Instrumentation Event Subscription		Indicator Blocking							
Registry Run Keys / Start Folder		Software Packing							
Change Default File Association		Masquerading							
Component Firmware		Obfuscated Files or Information							
Bootkit		Binary Padding							
Hypervisor		Install Root Certificate							
Logon Scripts		Network Share Connection Removal							
Modify Existing Service		Rootkit							
		Scripting							

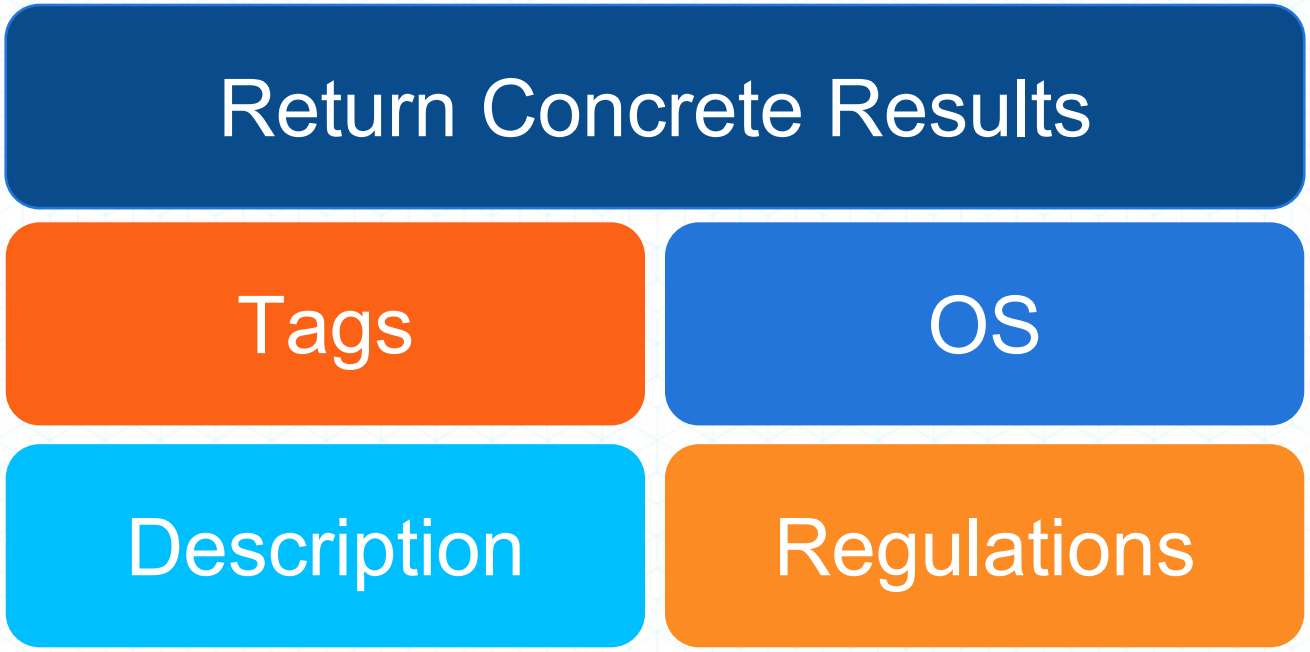
attack.mitre.org

Applying queries to frameworks

Common framework themes

- Firewall
- Credentials
- Access to data
- Access to critical systems
- Versions
- Account mgt
- Asset mgt
- Risk assessment
- Supply chain risk mgt
- IDAM risk
- Data security
- Anomalies and Events
- Security monitoring
- Filesystem config/permissions
- FIC
- Process hardening
- Access control
- Services
- Network config
- Logging and retention
- Remote access
- Removable media

Query requirements



Matrix Examples

Query Matrix

Network Access	User Access	Applications	Data Access	Risk Control
Firewall	Credentials	Versions	Access to data	Risk assessment
Filesystem config/permissions	Account mgt	Services	Removable media	Supply chain risk mgt
Access control		Process hardening	FIC (FIle integrity check)	Security monitoring
Network config		Asset mgt	Anomalies and Events	IDAM risk
Logging and retention			Data security	
Remote access			Access to critical systems	

Query Matrix: NIST

Bucket 1	Bucket 1	Bucket 3	Bucket 4	Bucket 5
Firewall	Credentials	Versions	Access to data	Risk assessment
Filesystem config/permissions	Account mgt	Services	Removable media	Supply chain risk mgt
Access control		Process hardening	FIC (FIle integrity check)	Security monitoring
Network config		Asset mgt	Anomalies and Events	IDAM risk
Logging and retention			Data security	
Remote access			Access to critical systems	

PR.AC-5: Network integrity protected

DE.CM-1: Network is monitored

DE.CM-7: Monitoring unauth. personnel

PR.DS-2: Data-in-transit protected

PR.DS-6: Integrity-checking mech.

Carbon Black.

Query Matrix:

Bucket 1	Bucket 1	Bucket 3	Bucket 4	Bucket 5
Firewall	Credentials	Versions	Access to data	Risk assessment
Filesystem config/permissions	Account mgt	Services	Removable media	Supply chain risk mgt
Access control		Process hardening	FIC (FIle integrity check)	Security monitoring
Network config		Asset mgt	Anomalies and Events	IDAM risk
Logging and retention			Data security	
Remote access			Access to critical systems	

1.4: Personal firewall actively running

1.3.6: Access to systems

4.1: Strong cryptography & protocols

11.5.a: Verify change-detection mech.

Carbon Black.

Individual tiles

Firewall

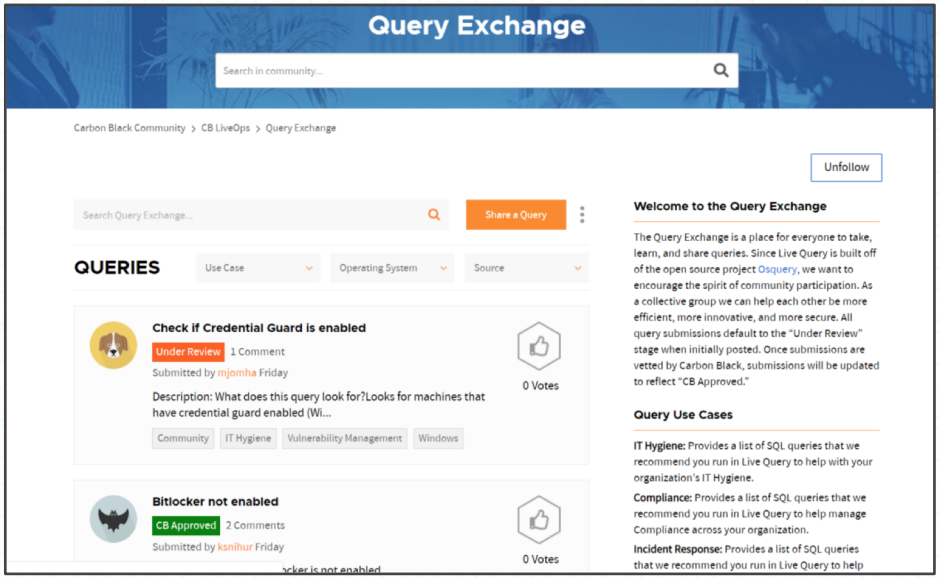
tag tag tag tag

The queries here are designed to detect certain configurations on host based firewalls that are potentially malicious, or bring you out of compliance

Query	OS	Description	Regulation
select * from foo	Windows	Blah, blah, blah	PCI 3.2.3 NIST 2.3.1
select * from bar	Mac, Linux	Blah, blah, blah	CIS 4.5 NIST 2.3.1 ATT&CK T1109, T13230
select * from baz	Windows, Mac, Linux	Blah, blah, blah	HIPPA 1.1

The Way Forward

Next steps



https://community.carbonblack.com/t5/Query-Exchange/idb-p/query_exchange

Carbon Black.

Discussion

Carbon Black.

www.CarbonBlack.com