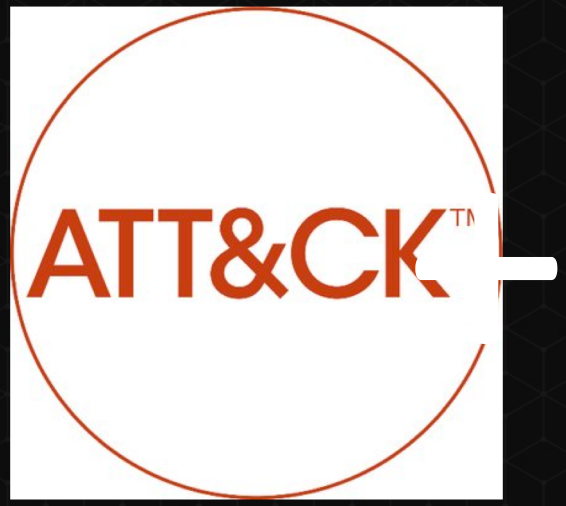

ATT&CK & OSQuery

Scott Lundgren @5twenty9

Carbon Black.

MY PATH

OPERATING SYSTEM DEVELOPER

OFFENSIVE RESEARCHER

PEN TESTER

CHIEF ARCHITECT @ CARBON BLACK

BUT WHERE AM I COMING FROM?

I BELIEVE ATT&CK IS A POSITIVE DEVELOPMENT.

I WISH FOR **SUSTAINED SUCCESS**

Carbon Black.

WHAT IS THE TIMEFRAME?

FUTURE

Carbon Black.

TEN MINUTES… GO!

1. ASSERT A **CHALLENGE**
2. INTRODUCE **OSQUERY**
3. PROPOSE A **CONVERSATION**

Carbon Black.

THE COMBINATION OF **TECHNICAL COMPLEXITY** AND **COMPETITIVE LANDSCAPE** POSES A LONG-TERM THREAT TO THE ATT&CK FRAMEWORK

INTRODUCING OSQUERY

Carbon Black.

ASSERTION: ATT&CK NEEDS AN ECOSYSTEM

- TESTING FRAMEWORKS ARE ABSOLUTELY THE FIRST STEP
- REFERENCE DETECTION IMPLEMENTATIONS ARE THE NEXT

Carbon Black.

INTRODUCING OSQUERY

- DEVELOPED BY FACEBOOK
- ENDPOINT AGENT
- OPEN-SOURCE
- EXTENSIBLE
- CROSS-PLATFORM

A SQL FRONT-END FOR ENDPOINT TELEMETRY

- 226+ TABLES
- ENDPOINT AGENT
- OPEN-SOURCE
- CROSS-PLATFORM

- arp_cache
- listening_ports
- logged_in_users
- kernel_modules
- rpm_packages
- scheduled_tasks
- bitlocker_info
- autoexec
- process_open_files
- process_open_sockets

Carbon Black.

PROPOSING THE CONVERSATION

Carbon Black.

THREE-LEGGED STOOL

ATT&CK FRAMEWORK

OPEN TESTING FRAMEWORK

OPEN REFERENCE DETECTIONS

Carbon Black.

EXISTING REFERENCE DETECTION IMPLEMENTATIONS

FILIPPO MOTTINI, OLAF HARTONG, POLYLOGX

Olaf Hartong
olafhartong

Code | Issues 3 | Pull requests 0 | Projects 0 | Wiki

Branch: master ▾ osq-ext-bin / README.md

polylogyx Update README.md

1 contributor

171 lines (124 sloc) | 7.75 KB

1. PolyLogyx osquery Extension for Windows

PolyLogyx OSQuery Extension (plgx_win_extension.ext.exe) for Windows pl
adding real time event collection capabilities to osquery on Windows platfo
services library of PolyLogyx. The current release of the extension is a 'con
aimed at increasing osquery footprint and adoption on Windows platform. \
Windows kernel for osquery, the possibilities can be enormous.

Pinned Tweet

filippo mottini @teoseller ·
Here my project of mapping
github.com/teoseller/osqu.

Code | Issue | sights

Branch: master ▾ osquery-attck / network_connection_listening.conf

Find file | Copy path

teoseller Update network_connection_listening.conf 277c025 6 days ago

1 contributor

35 lines (33 sloc) | 1.88 KB | Raw | Blame | History

```
{
  "queries": {
    "Windows_Process_Network_Conn": {
        "query": "select DISTINCT p.name, p.path, pos.remote_address, pos.remote_port from process_open_sockets pos LEFT JOIN
        "interval": 60,
        "description": "Returns the network connections from system processes - ATT&CK T1086,T1093,T1020,T1041,T1011,T1029,T10
```

```
<Sysmon schemaversion="4.0">
  <!-- Capture all hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <CheckRevocation/>
  <EventFiltering>
    <!-- Event ID 1 == Process Creation. -->
    <ProcessCreate onmatch="exclude">
    <!--SECTION: Microsoft:Office:Click2Run-->
    <Image condition="is">C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</Image> <!--Microsoft:Office: Background process-->
    <ParentImage condition="end with">C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe</ParentImage> <!--Microsoft:Office: Background process-->
    <ParentImage condition="is">C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</ParentImage> <!--Microsoft:Office: Background process-->
    </ProcessCreate>
```

Carbon Black.

PUTTING FORWARD OSQUERY

- OPEN
- EXTENSIBLE
- CROSS-PLATFORM
- APPROACHABLE

```
SELECT * FROM T1197;
```


Carbon Black.

THINK & CONVERSE

Carbon Black.