# ATT&CK @ Cegeka

# whoami

SECURITY ANALYST
CEGEKA SOC

BELGIUM, HASSELT

BEER & PIZZA
(BAKING) ENTHUSIAST

SVEN.JACOBS@CEGEKA.COM

IG: @THEBEERBAKER.EU

SWIMMING & CYCLING

+25 years

A TRUSTED IT-PARTNER

+2,500

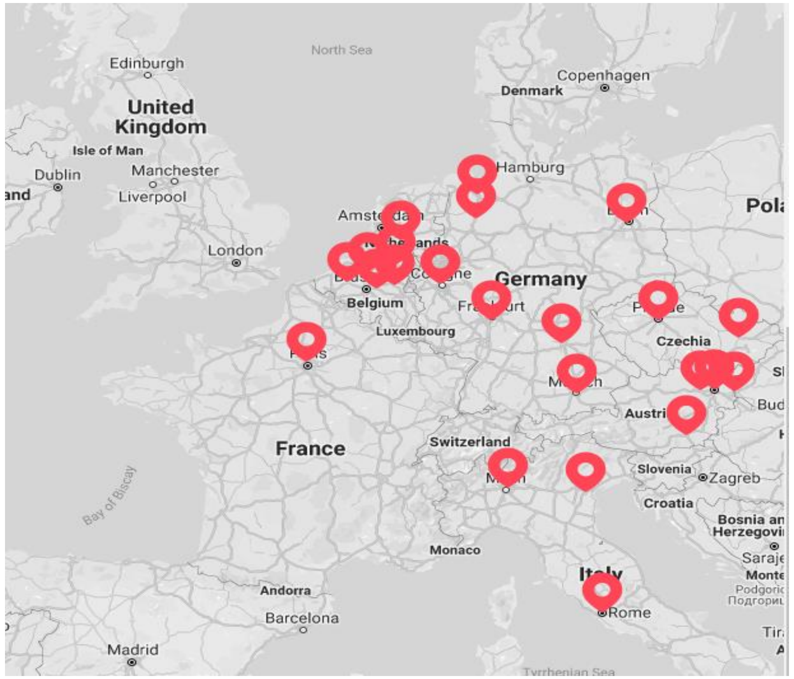
HAPPY CUSTOMERS

+20

EUROPEAN OFFICES

+4,200

ENGAGED EMPLOYEES



# Cegeka

Founded 1988

IT-partner in:

- Software
- Hybrid Cloud Solutions
- Outsourcing
- Data & Automation
- Digital

# Cegeka SOC

- Vulnerability & Hardening Management
- Incident Response
- Security Monitoring
- Threat Intelligence
- Penetration testing
- Risk Assessments
- Consulting
- Phishing / Social Engineering Attacks

# How ATT&CK Unfolded

Mentioned during a training a couple of years ago…

Immediate benefit:

Tuned our monitoring use cases

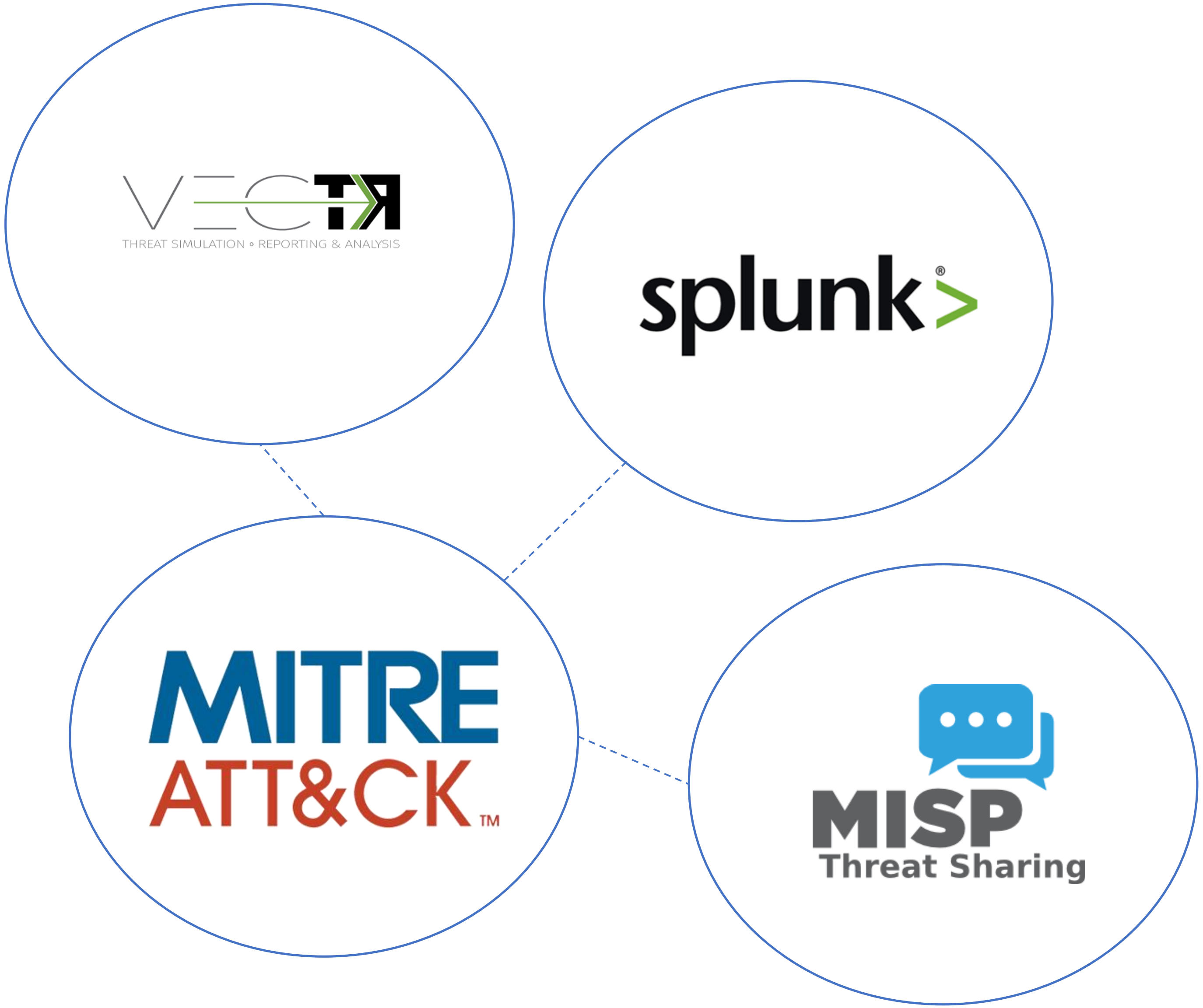
Response after first use:

Must embed in other processes

# Detection

## ATT&CK – use case

# Detection

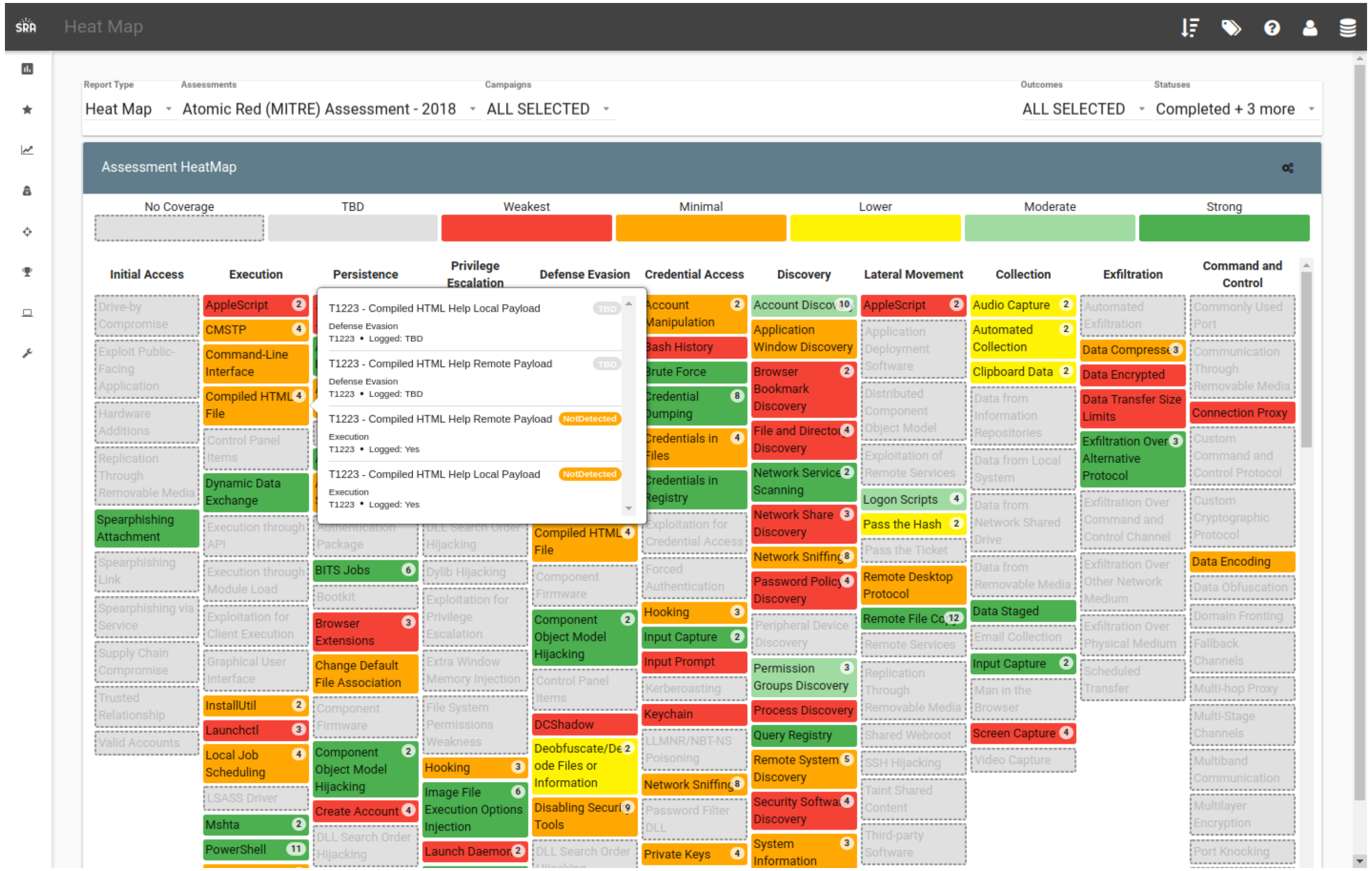

VECTR
THREAT SIMULATION ∘ REPORTING & ANALYSIS
splunk>
MITRE
ATT&CK™
MISP
Threat Sharing

# Detection

Quality checks on capabilities with VCTR*

https://github.com/SecurityRiskAdvisors/VECTR

VECTR
THREAT SIMULATION • REPORTING & ANALYSIS



Report Type: Heat Map
Assessments: Atomic Red (MITRE) Assessment - 2018
Campaigns: ALL SELECTED
Outcomes: ALL SELECTED
Statuses: Completed + 3 more

Assessment HeatMap

No Coverage | TBD | Weakest | Minimal | Lower | Moderate | Strong

**Initial Access**
- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

**Execution**
- AppleScript 2
- CMSTP 4
- Command-Line Interface
- Compiled HTML File 4
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil 2
- Launchctl 3
- Local Job Scheduling 4
- LSASS Driver
- Mshta 2
- PowerShell 11

**Persistence**
- Authentication Package
- BITS Jobs 6
- Bootkit
- Browser Extensions 3
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking 2
- Create Account 4
- DLL Search Order Hijacking

**Privilege Escalation**
- DLL Search Order Hijacking
- Dylib Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking 3
- Image File Execution Options Injection 6
- Launch Daemon 2

**Defense Evasion**
- Compiled HTML File 4
- Component Firmware
- Component Object Model Hijacking 2
- Control Panel Items
- DCShadow
- Deobfuscate/Deode Files or Information 2
- Disabling Securi Tools 9
- DLL Search Order Hijacking

T1223 - Compiled HTML Help Local Payload TBD
Defense Evasion
T1223 • Logged: TBD

T1223 - Compiled HTML Help Remote Payload TBD
Defense Evasion
T1223 • Logged: TBD

T1223 - Compiled HTML Help Remote Payload NotDetected
Execution
T1223 • Logged: Yes

T1223 - Compiled HTML Help Local Payload NotDetected
Execution
T1223 • Logged: Yes

**Credential Access**
- Account Manipulation 2
- Bash History
- Brute Force
- Credential Dumping 8
- Credentials in Files 4
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking 3
- Input Capture 2
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning
- Network Sniffing 8
- Password Filter DLL
- Private Keys 4

**Discovery**
- Account Discov 10
- Application Window Discovery
- Browser Bookmark Discovery 2
- File and Directo Discovery 4
- Network Service Scanning 2
- Network Share Discovery 3
- Network Sniffing 8
- Password Policy Discovery 4
- Peripheral Device Discovery
- Permission Groups Discovery 3
- Process Discovery
- Query Registry
- Remote System Discovery 5
- Security Softwa Discovery 4
- System Information 3

**Lateral Movement**
- AppleScript 2
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts 4
- Pass the Hash 2
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Co 12
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software

**Collection**
- Audio Capture 2
- Automated Collection 2
- Clipboard Data 2
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture 2
- Man in the Browser
- Screen Capture 4
- Video Capture

**Exfiltration**
- Automated Exfiltration
- Data Compresse 3
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol 3
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

**Command and Control**
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking

# Reporting

## ATT&CK – use case

# Reporting

**ATT&CK advantages:**

- Report on environments
  - ➢ Steer your security defenses more easily
  - ➢ Improves existing security reporting

- Making risks tangible again …
  - ➢ Useful to build a business case
  - ➢ Convince other teams on certain facts

- Good structure for incident write-ups

MISP Heat Map

Cloud ATT&CK

# ATT&CK – future