Red Team Village at DEF CON 32

Adversary Simulation: Using Blue Eyes to See Red

Friday, August 9, 2024 1:00 pm

Fred Wilmot

Sebastien Tricaud

$whoami

Sebastien Tricaud

Co-founder, Detecteam
Director of Security Research at Devo.
Security Researcher at Splunk.
Developer of Faup URL Parser, MISP SightingsDB, Linux PAM, Prelude IDS
Former CTO of Honeynet Project

Fred Wilmot

- Co-founder, Detecteam
- Wrote ICS/SCADA protocol signatures on power distribution systems for DoE
- Founded Splunk’s Security practice
  Co-founded Red Team Offensive Village and Texas Cyber Summit
- Managing Principle with AMCyber Red Team Research
- KCBsides conspirator

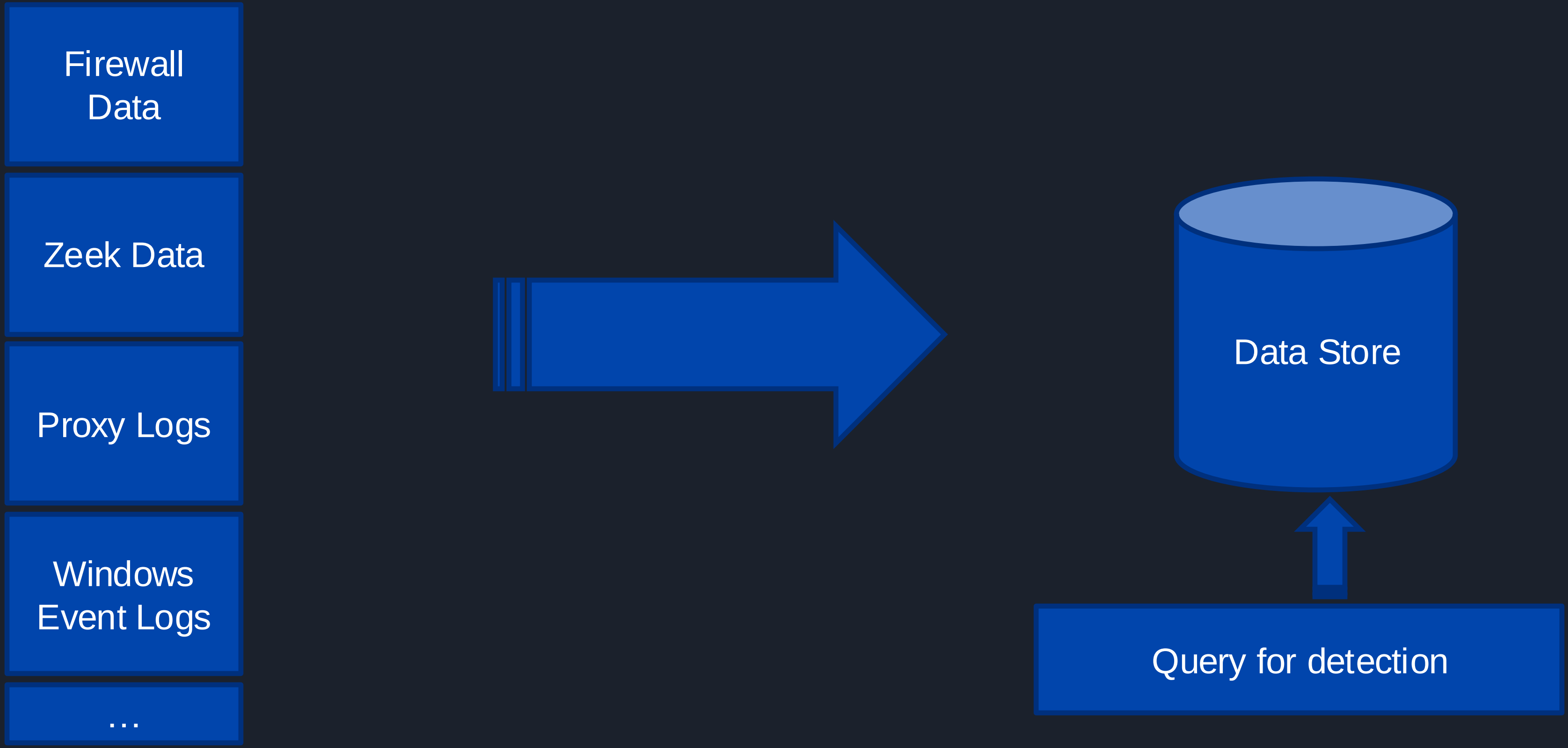
Problem

Red Team Goals: For an attack scenario, I want to bypass detections

- Specific Adversary behavior toolsets
  - Atomic Red Team
    - Uses Hypothesis (python)
    - Pydantic (python)
  - Faker project
  - Platform IDE
  - Home brewed Powershell and/or Python script?
  - ADEL as a language
- Crafting Attack scenarios and commercial detections <Detecteam Testbench>
  - Only presents one side of the ecosystem view – I want to know what gets detected and mutate the attack
  - Improving Scenario quality – binary inclusions, technology types, data models, action types, tactics, behavior and performance.

Hypothesis testing without feedback is hard

Detection from a Log Ingestion



Firewall Data

Zeek Data

Proxy Logs

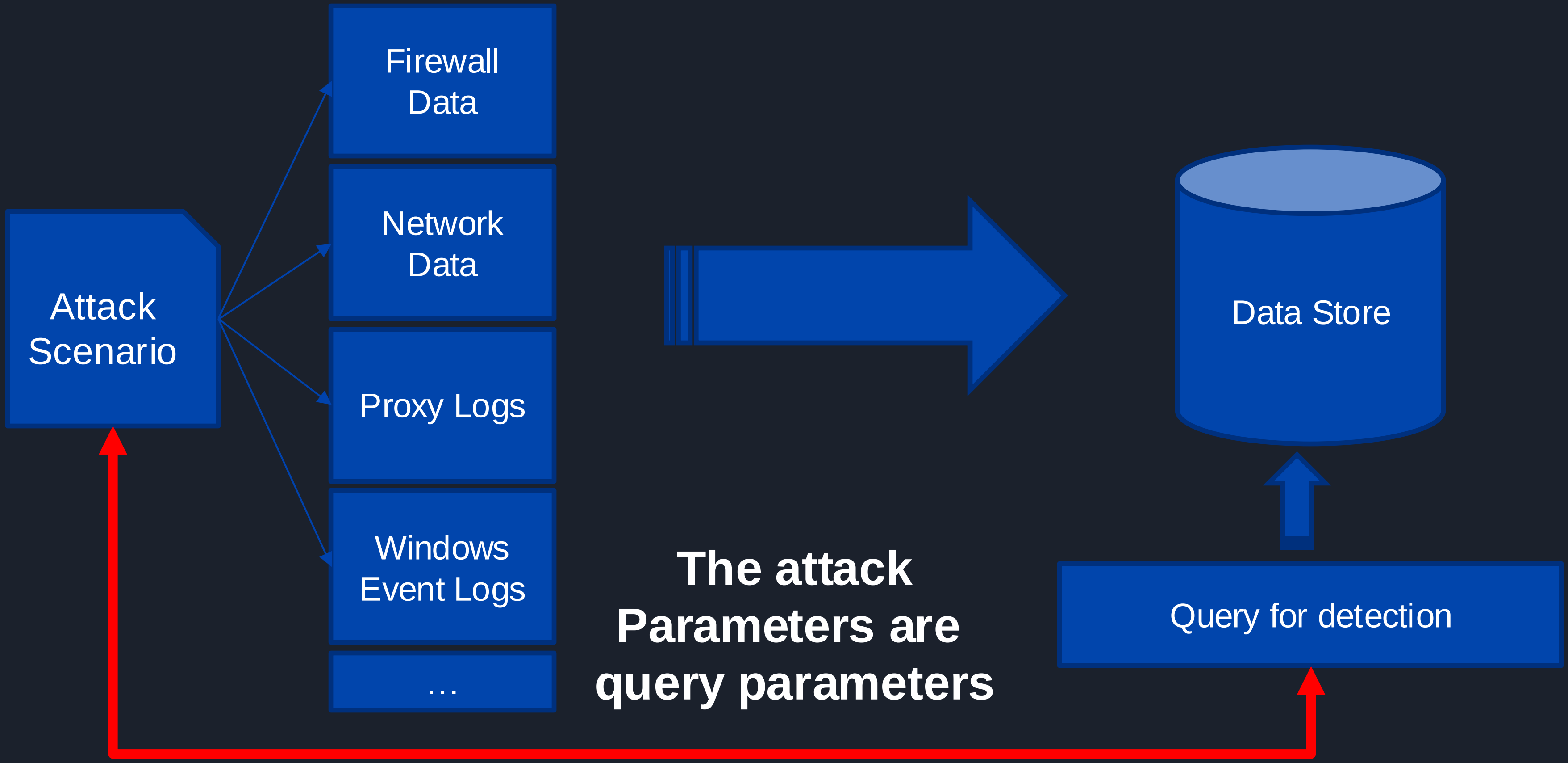
Windows Event Logs

…

Data Store

Query for detection

Attack Behavior Define Detections

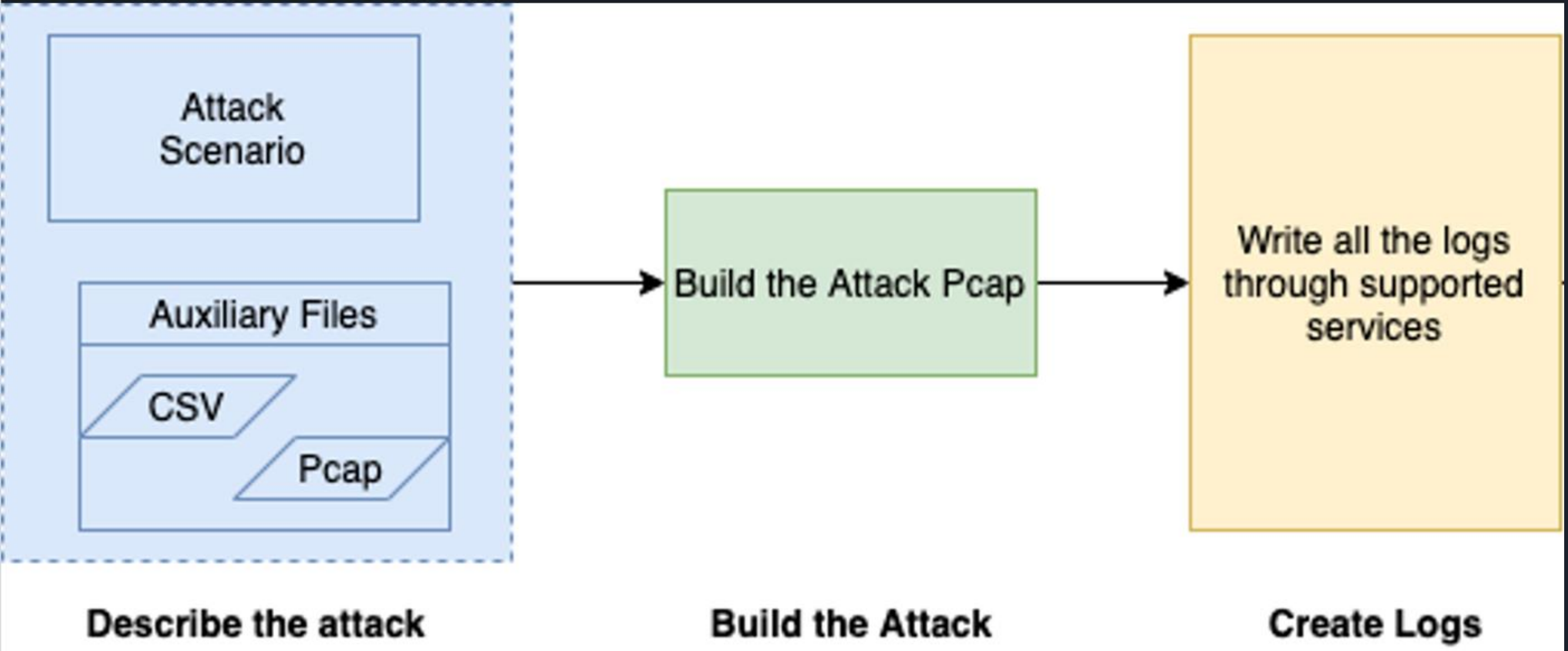


The attack Parameters are query parameters

Red Team Village Community Edition

“Free as in Beer” Detecteam platform instance: collaborate on scenarios, PCAPs, STIX objects, and detections

- http://Detecteam.io
  - community@Detecteam.com email with name, email, role. [validation required]
  - Set up MFA – tenant isolation
  - Configure integration to send data
- Github Repos (Open Source / tenant-specific)
  - https://github.com/adel-lang/scenarios
  - <plug in your github repo>
- Executing Scenarios
  - Integrations – define and configure <Elastic Free Trial>
  - Validating the trigger and the slip



Attack Scenario

Auxiliary Files

CSV

Pcap

Build the Attack Pcap

Write all the logs through supported services

Describe the attack

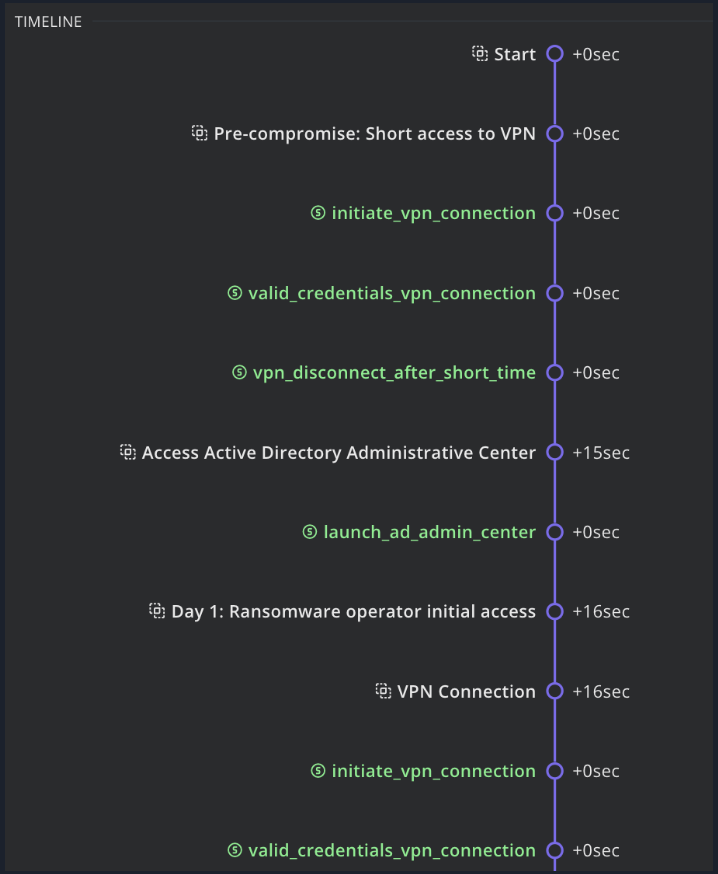
Build the Attack

Create Logs

Attack Description Language

Introducing ADEL

- JSON definitions
- Sections & Steps
- Runs & Actions
- Tactics & Techniques
- Scenario Variables
- scenario-as-code
- Hypothesis-based testing



TIMELINE

Start +0sec

Pre-compromise: Short access to VPN +0sec

initiate_vpn_connection +0sec

valid_credentials_vpn_connection +0sec

vpn_disconnect_after_short_time +0sec

Access Active Directory Administrative Center +15sec

launch_ad_admin_center +0sec

Day 1: Ransomware operator initial access +16sec

VPN Connection +16sec

initiate_vpn_connection +0sec

valid_credentials_vpn_connection +0sec

Building a Scenario

Examples: Sections, Steps, Functions, Features

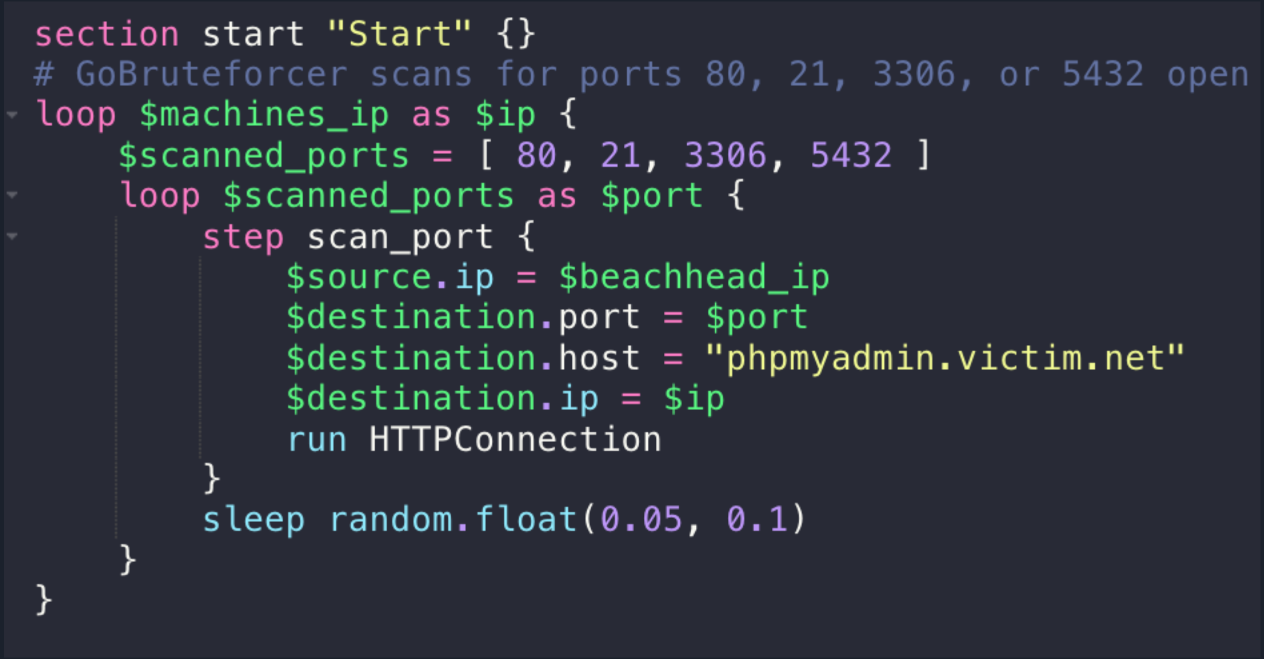
Describe Adversary behavior

Basics

- Building Blocks

- sections are tactics
- Steps are techniques

More advanced -
Scenarios from PCAPs,
STIX Objects, Detections



```
section start "Start" {}
# GoBruteforcer scans for ports 80, 21, 3306, or 5432 open
loop $machines_ip as $ip {
    $scanned_ports = [ 80, 21, 3306, 5432 ]
    loop $scanned_ports as $port {
        step scan_port {
            $source.ip = $beachhead_ip
            $destination.port = $port
            $destination.host = "phpmyadmin.victim.net"
            $destination.ip = $ip
            run HTTPConnection
        }
        sleep random.float(0.05, 0.1)
    }
}
```

Show the all the things...

Red Team Village Community Edition

“Free as in Beer” Detecteam platform instance: collaborate on scenarios, PCAPs, STIX objects, and detections

- http://Detecteam.io
  - community@Detecteam.com email with name, email, role. [validation required]
  - Set up MFA – tenant isolation
  - Configure integration to send data
- Github Repos (Open Source / tenant-specific)
  - https://github.com/adel-lang/scenarios
  - <plug in your github repo>
- Executing Scenarios
  - Integrations – define and configure <Elastic Free Trial>
  - Validating the trigger and the slip

Thank You

community@Detecteam.com

https://detecteam.io