ATT&CK Simulation - democratizing the red team toolkit for all defenders

April 2024

Mitch Ryan
APAC Security Solution Architect
Splunk

splunk> a cisco company

Agenda

- Why I’m here
- ATT&CK simulation
- How Splunk does it internally
- A practical application

splunk> a CISCO company

Mitch Ryan

- Splunk Senior Security Solution Architect - APAC
- ~17 years in Enterprise technology
- Focused on securing highly targeted sectors
  - Government
  - FSI
  - Healthcare
- How I leveraged automated Attack Simulation…

Attack Simulation – a definition

Use attack techniques against network, system, processes

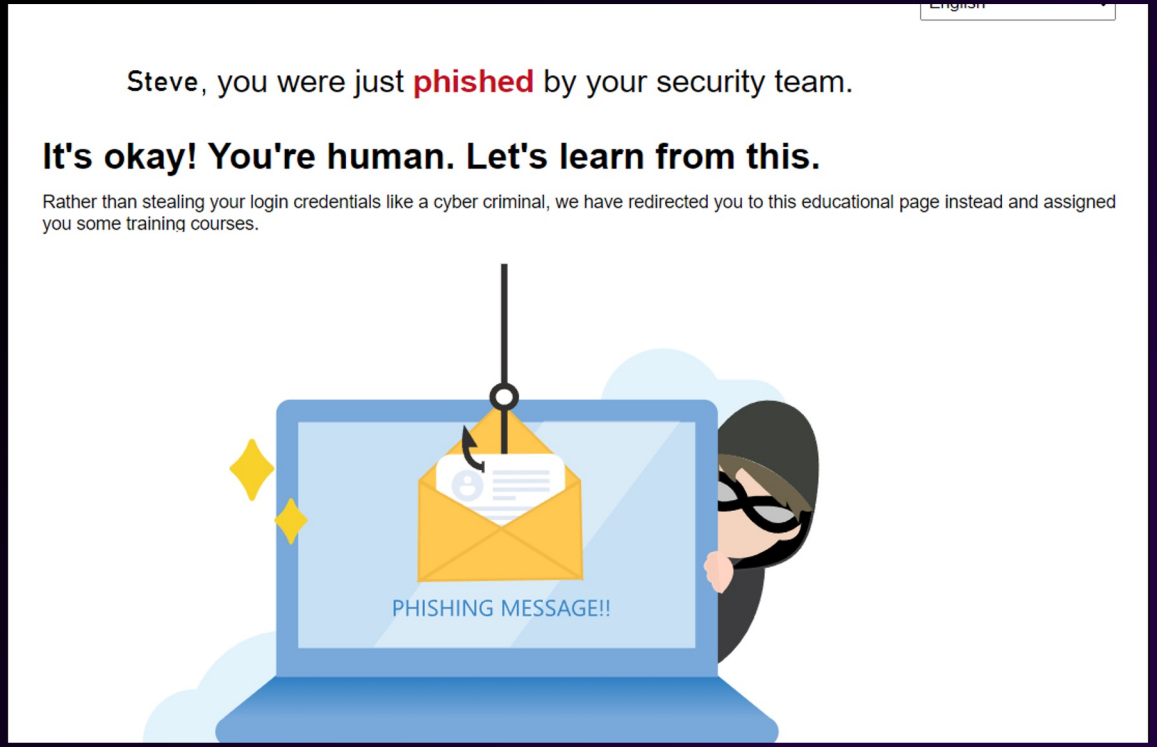
Used to test defences, iteratively improve systems

Part of threat informed defence, and assume breach

Intended to improve security posture, knowledge

splunk>

A common attack simulation technique



How does Attack Simulation and MITRE help you?

Levels playing field

Shift from reactive to proactive

Exposure to diverse threats / develop skills / learn to hunt

Consistency and common language

splunk>

Open source to the rescue

Some options – plenty more exist

https://github.com/splunk/attack_range

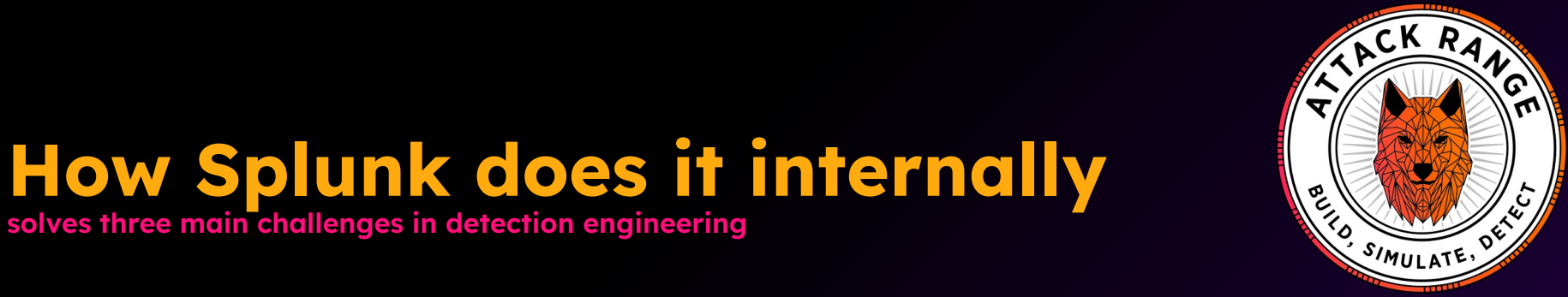
https://github.com/mitre/caldera

https://github.com/center-for-threat-informed-defense/adversary_emulation_library

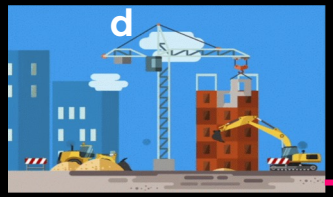
https://github.com/guardicore/monkey

How Splunk does it internally

solves three main challenges in detection engineering



Buil d



Quickly build a small lab infrastructure as close as possible to a production environment that is fully configured.

Simulate

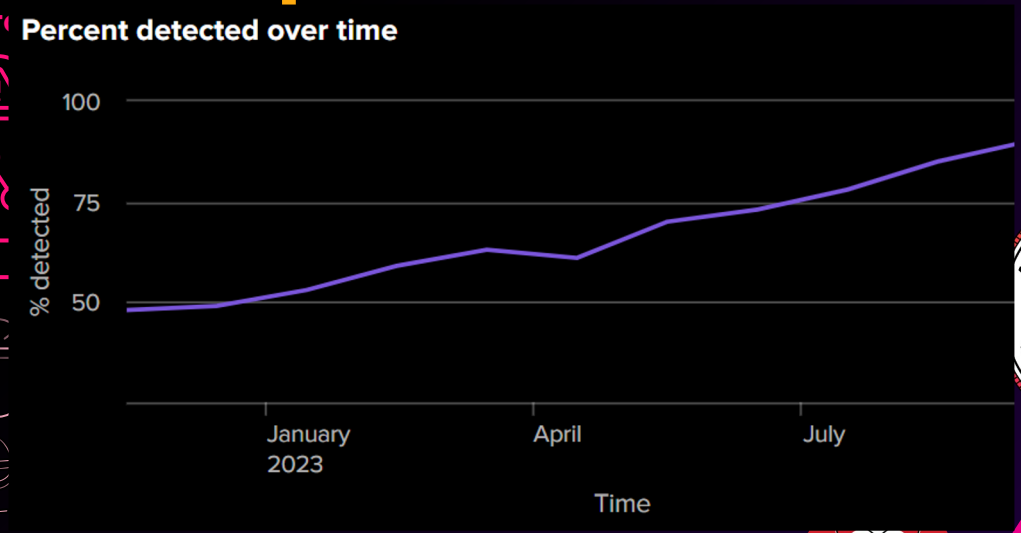
The Attack Range performs attack simulation using different engines such as Atomic Red Team or Prelude Operator in order to generate real attack data.

Test

It integrates seamlessly into any Continuous Integration / Continuous Delivery (CI/CD) pipeline to automate the detection rule testing process.

How it works in practice

Leverage MITRE ATT&CK t



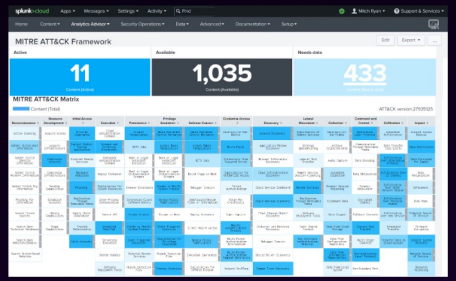
splunk>

ATTACK RANGE
BUILD, SIMULATE, DETECT

CALDERA

Threat Feed

Commercial/Open Source, Hypothesis Led, MITRE ATT&CK based



Attack Simulation

Manual/Automated, fire attack at system to assess detection

Detection Engineering Cycle

Detection Reporting

MITRE heatmap, % simulated attacks detected

Build/refine detection if required

ATTACK RANGE

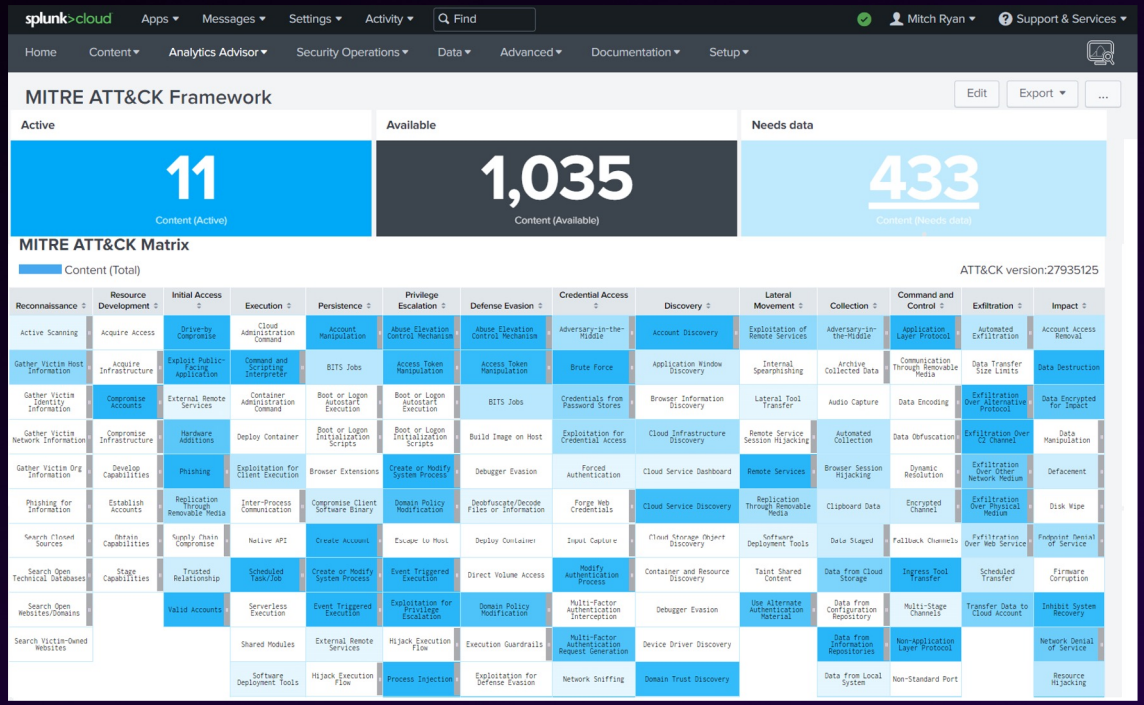
BUILD, SIMULATE, DETECT

Security Essentials

Security content library

Browse, bookmark, and deploy 1700+ security detections and analytic stories

- Repository of Security Content for Splunk Cloud, Enterprise Security, UEBA, and SOAR
- Deploy security content within clicks
- Enrich notable events and run analytics with context from content library
- Stay up to date on ransomware + emerging threats



splunk> a cisco company

Thank you!