Reframing Attack Path Analysis for Cloud Risk Assessment

February 26, 2025

Jon King

You may remember me from past successes as…

- Husband, father, veteran
- IT and InfoSec Admin, Engineer, Architect, and Manager
- InfoSec Consultant and Speaker

Agenda

- Warm Up
- Risk in the Cloud
- Attack Path Analysis
- Logistics & Operations
- Example

Warm Up

Fill in the ______!

MITRE ______

Cyber Defense ______

Cyber Security First __________

Quantitative ____ Analysis

How to _______ Anything in Cybersecurity Risk

The _______ Project

Tactics, Techniques, & __________

_______ of Pain

Get to the *right* questions

Risk in the Cloud

Cybersecurity Risk in the Cloud

- Cloud adoption & its evolving threat landscape
- Shared responsibility model
- Importance of continuous risk assessment
- Layered Defenses, Zero-Trust, & Guardrails

Protect Surfaces in the Cloud

- Defining Protect Surfaces
- Protect surfaces as “micro-environments”
- Visibility into protect surfaces
- Executive vs. Administrator vs. Engineer vs. Architect

Contextualizing the answers

Attack Path Analysis

Overview

- Review of Attack Path Analysis
- Conventional use for incident investigations
- Attack path analysis for active defenders

Attack Path Analysis for Cloud-Based Protect Surfaces

- Mapping possible paths an attacker might take in a protect surface
- Identifying critical nodes and choke points
- Prioritizing opportunities for improvement

Enabling meaningful insights

Logistics & Operations

Establish Inventories

- Asset Type Inventory
  - Virtual machines, containers, serverless functions, storage buckets, IAM roles, etc
- Inventory of controls & capabilities
  - Capabilities: Aspects that enable an organization’s resilience
  - Controls: Promises made by an organization about what they do

Map Known Threat Actor Behaviors to Asset Types

- Research threat actor TTPs (Techniques, Tactics, and Procedures)
- Align each TTP to specific asset types it typically affects
- Frameworks like ATT&CK, D3FEND, CWE, and OWASP Top 10 Lists help with consistent mapping

Map Controls & Capabilities to Known Threat Actor Behaviors

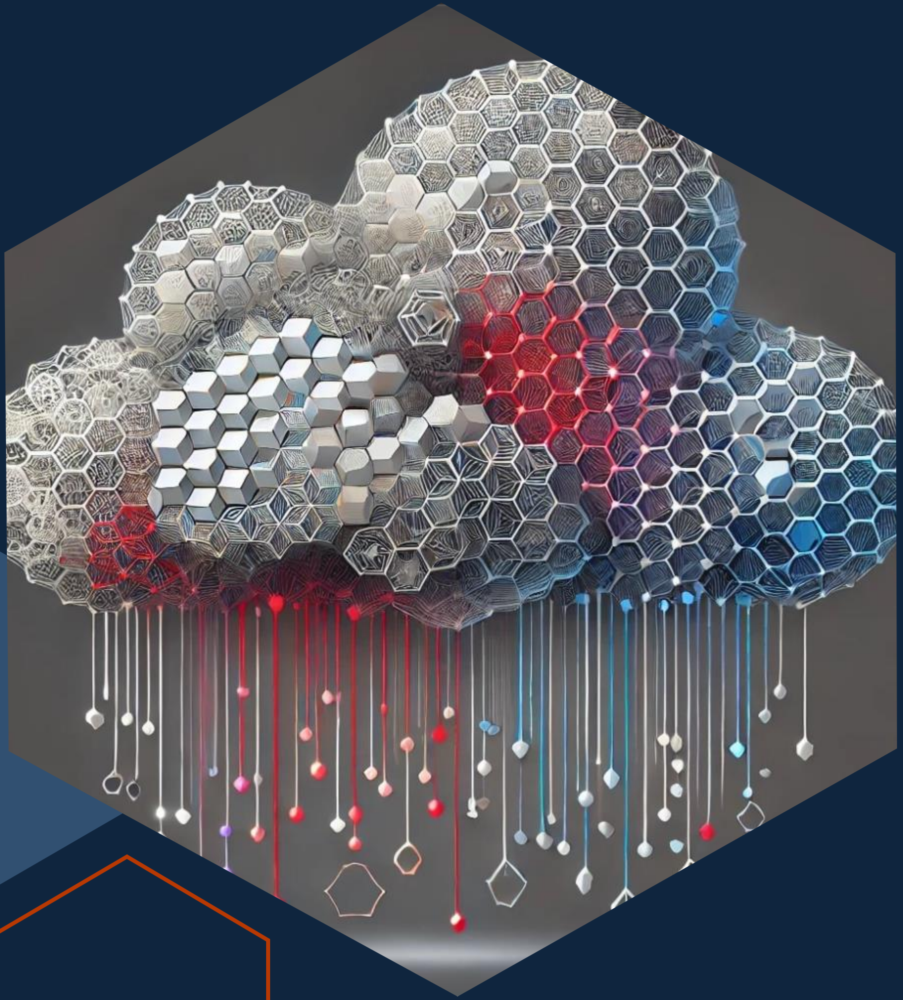
- Identify how each control mitigates or detects specific TTPs
- Assess overlap or gaps in controls (defense-in-depth vs. single points of failure)
- Example: IAM policies to protect against privilege escalation, or security observability to detect suspicious access

Define a Correlation Framework

- Correlate threat actor behaviors, asset types, and controls
- Build risk scenarios
  - Adversary emulation plans
  - Monte Carlo simulations
- Iterate and refine based on outcomes

In action

Example



Follow Along

https://github.com/illusconsulting/attack-shuffle-lite

https://illusconsulting.github.io/attack-shuffle-lite/

Thank you

Jon King

https://www.linkedin.com/in/jrkingitpro/