F5 & HashiCorp

SMOKE THE COMPETITION

CONTRATULATIONS

LEADERBOARD

Name	Partner	Total Points
Colby Canutt	Optiv	1200
Justin Stevens	Bridge Data	1200
Dave Unger	InterVision	800

Checkpoint 3 - Review

Question: How many pool members was Eric able to quickly scale up to at the end of the video using Consul Terraform Sync?

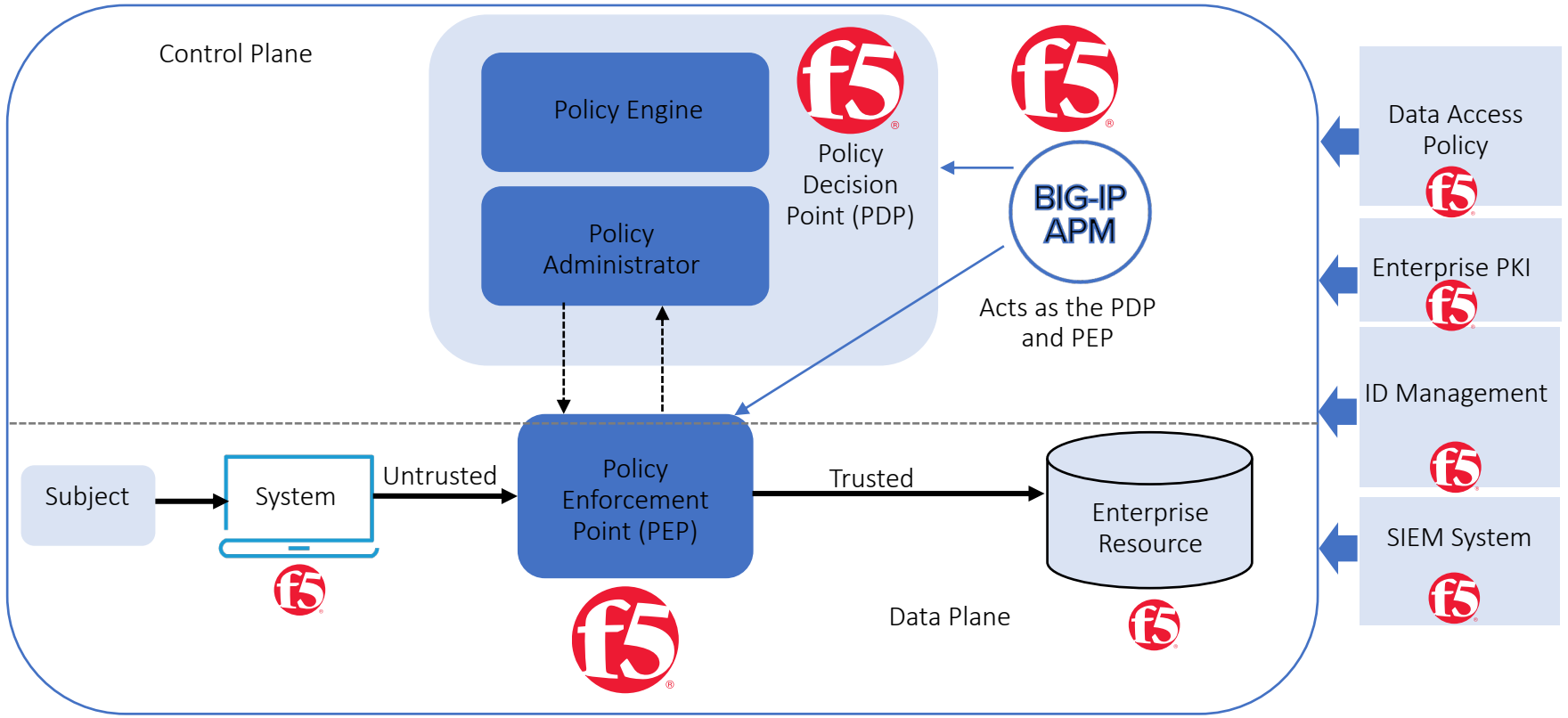
Answer - 100

Question: What did James forget to do?

Answer: He forgot to show the app actually working.

F5 Security Strategy for Zero Trust

F5 in the NIST Zero Trust Architecture

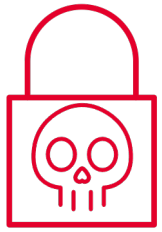


F5 addressing Zero Trust Threats

DoS / DDoS Attack(s)

Addressed by:

- F5 Advanced WAF
- NGINX App Protect
- NGINX App Protect L7 DoS
- Silverline WAF
- Silverline DDoS Protection
- Silverline Shape Defense
- BIG-IP AFM



Network Visibility / Encrypted Threats

Addressed by:

- F5 SSL Orchestrator

Stolen / Leaked Credentials

Addressed by:

- F5 Advanced WAF with Leaked Credential Check
- Shape Enterprise Defense
- Silverline Shape Defense

Storage of System / Network Info

Addressed by:

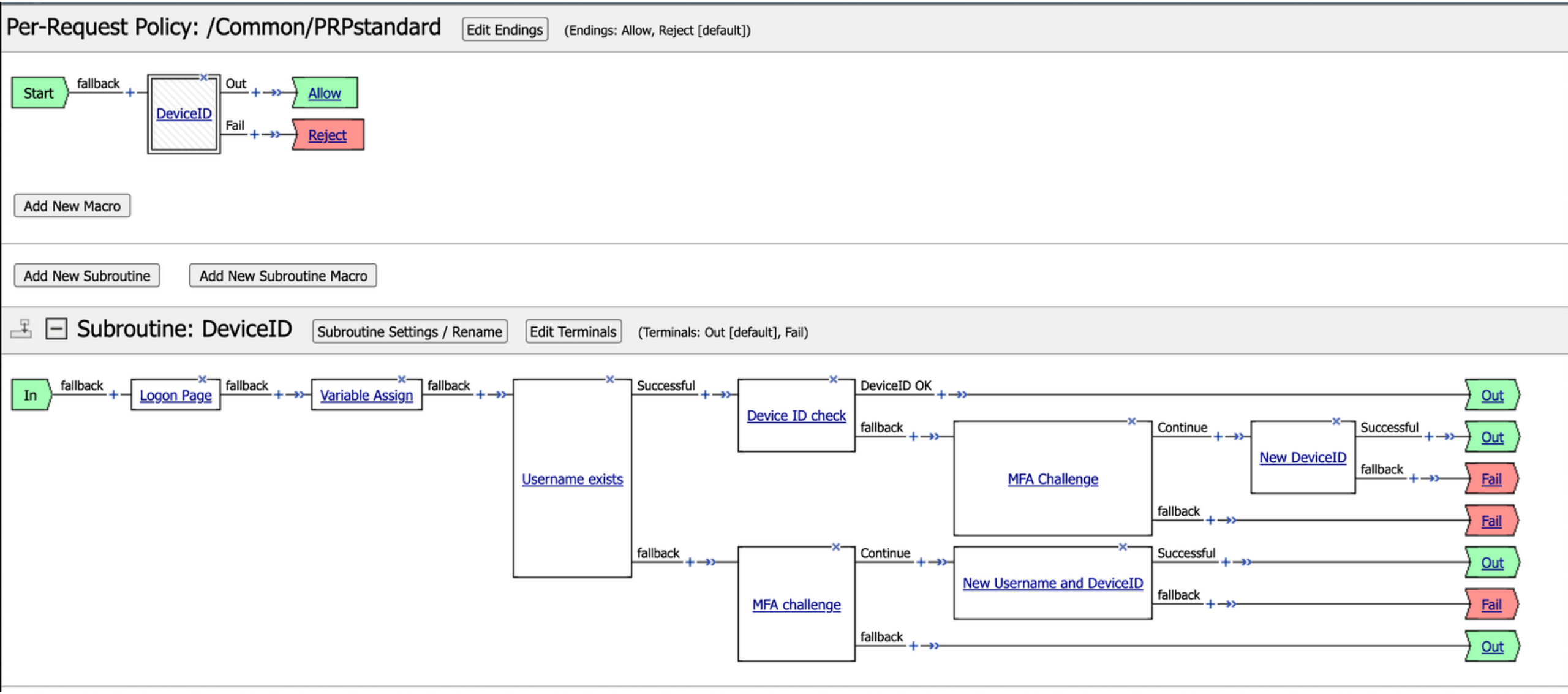
- BIG-IP APM
- F5 Advanced WAF
- Silverline WAF
- NGINX WAF
- BIG-IP AFM

Use of Non-person Entities (NPEs)

Addressed by:

- F5 Advanced WAF
- Silverline WAF
- NGINX App Protect
- NGINX Controller
- BIG-IP APM
- Volterra VoltMesh
- Aspen Mesh

Example Zero Trust Policy with DeviceID+

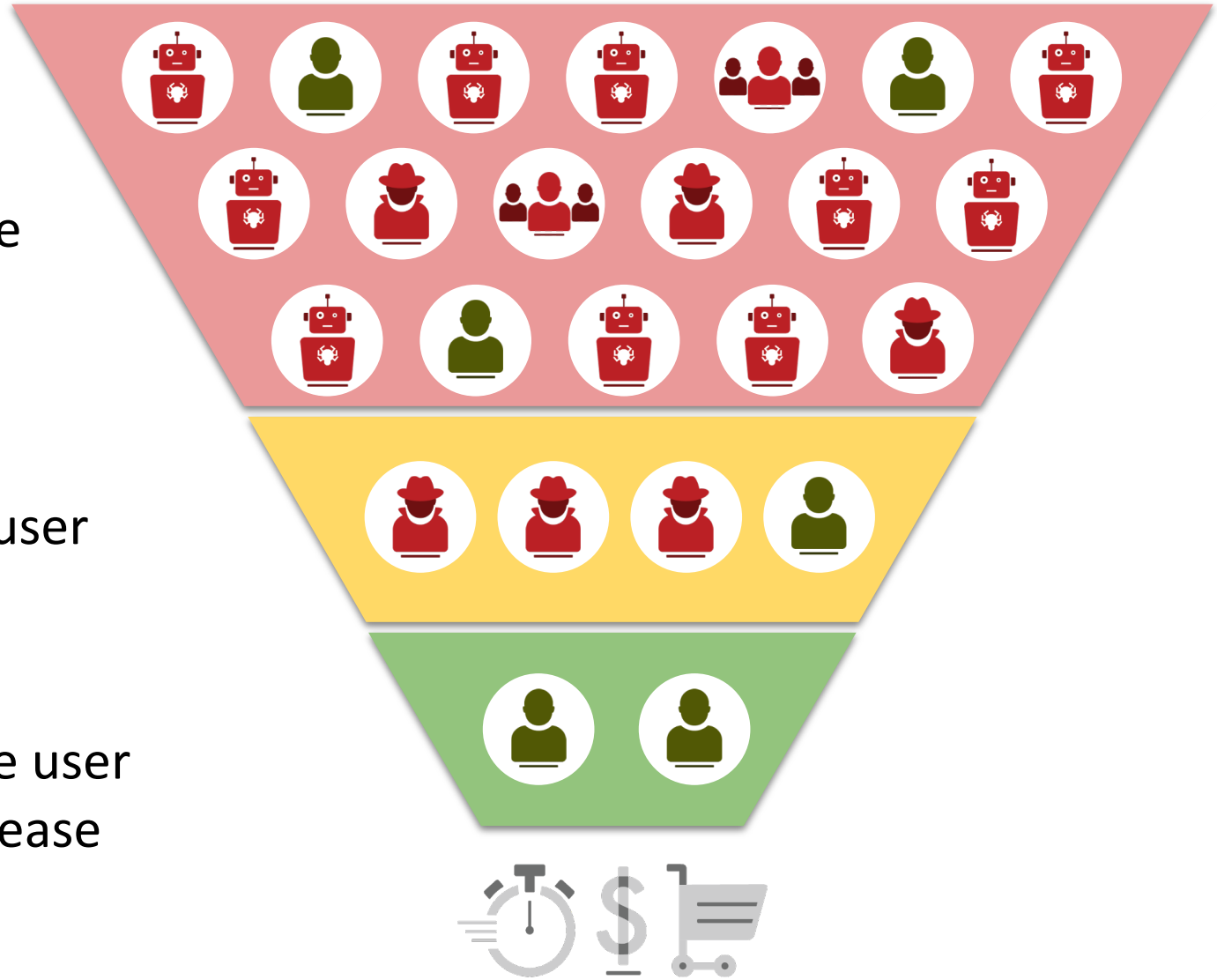


The Shape Platform

Enterprise Defense
Identify and mitigate unwanted traffic

SAFE
Identify fraudulent user behavior

Recognize
Create a friction free user experience and increase revenue



Bots

Human Clickfarm

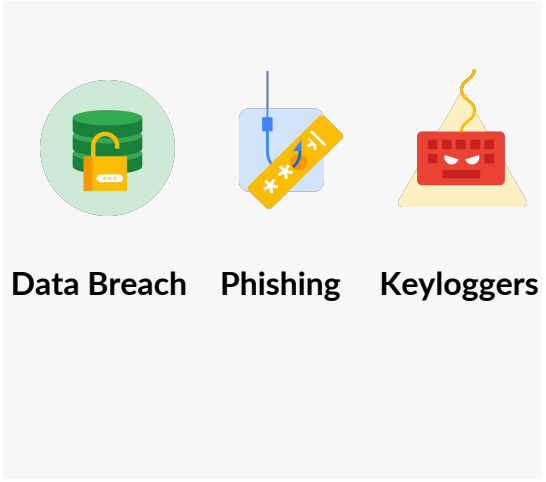
Manual Fraud Actors

Good Customers

The accelerated attack lifecycle

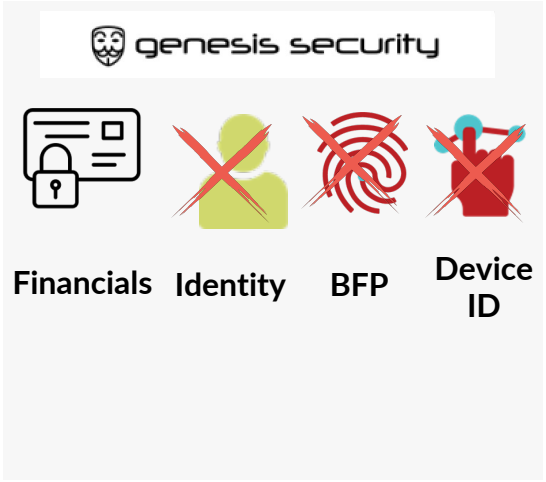
IT STARTS WITH UNWANTED AUTOMATION AND ENDS WITH ACCOUNT TAKEOVER AND APPLICATION FRAUD

Credentials are Stolen



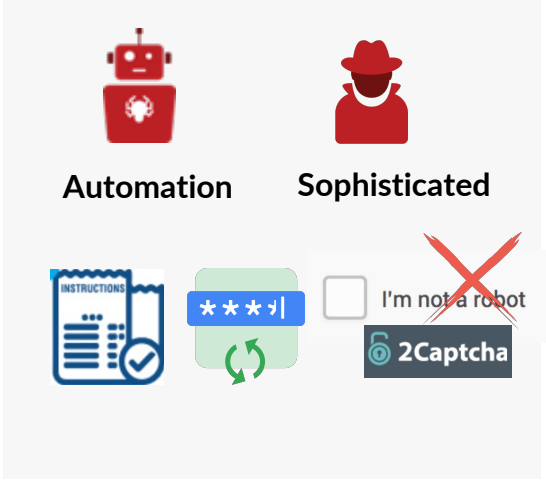
- Over 1 Million stolen credentials are reported every day

Stolen Credential Database is built



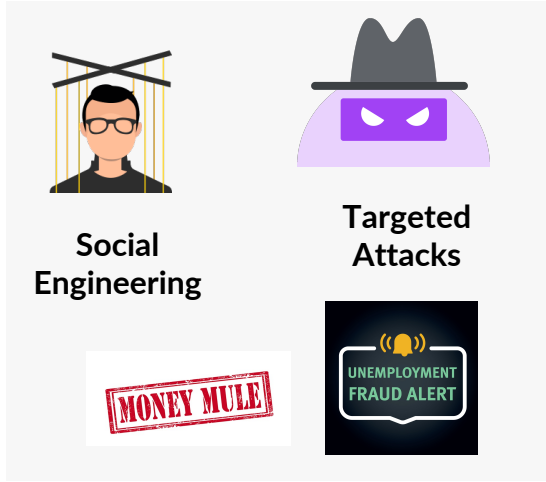
- The black market has industrialized cyber crimes and fraudulent activities

Accounts are Compromised



- Automation, malicious bots, and manual attacks expose users and businesses to fraud

Leading to Fraud & Friction



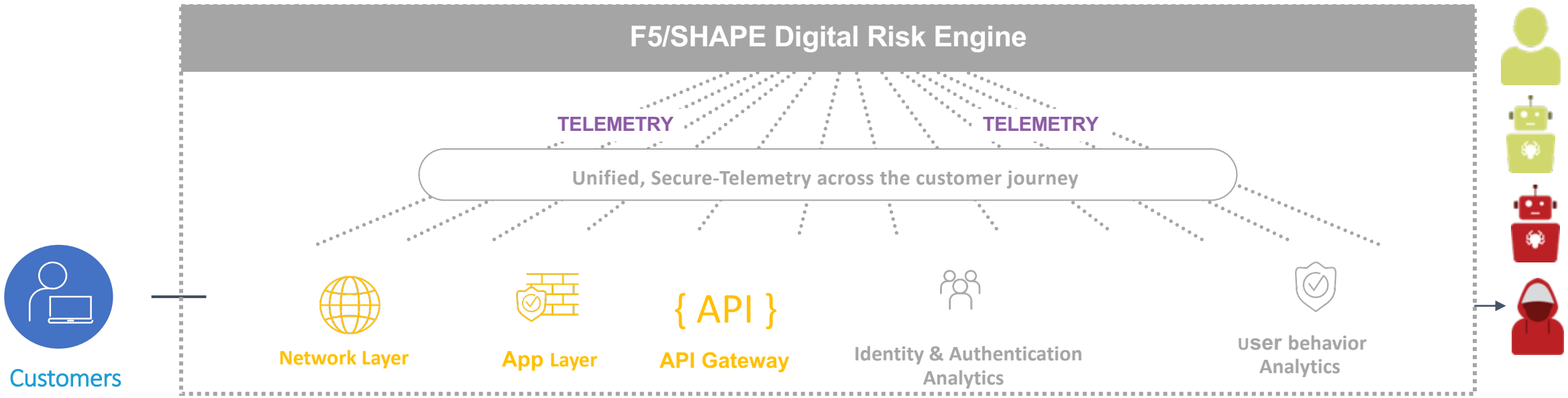
- Leading to 65% increase in successful fraud attempts from 2019 to 2020

The Future: Single view of customer trust & safety

Security
Secure Digital Experience

Risk
Reduce Fraud Loss

Business & Customer Exp
Increase Revenue



Signup Login Activity Transaction

SAFE delivers differentiated *outcomes* in *real-time*

Machine Learning models dynamically adapt to ever-changing fraudster human behaviors

LESS FRAUD

SAFE typically **identifies 2x-5x more fraud per month** than current solutions, while maintaining low false positive levels

LESS FRICTION

SAFE recommends **up to 90% FEWER MFA challenges** for legitimate users than alternative solutions - less user friction for legitimate users means more revenue

LESS EFFORT

SAFE slashes the # of transactions that require fraud team review **by more than 50%**

Typical SAFE Return on Investment: 6-10 *weeks*

HashiCorp

Zero-Trust with HashiCorp

https://www.hashicorp.com/solutions/zero-trust-security

The migration to cloud security

Traditional Datacenter

Static

Defend the Perimeter

+

Modern Datacenter

Dynamic

Inoculate the Interior

=

Defense in Depth

The migration to cloud security

Traditional Datacenter

Static

Defend the Perimeter

+

Modern Datacenter

Dynamic

Inoculate the Interior

=

Defense in Depth

Trust Nothing ...

- Identify and firewall everything
- Encrypt everything at rest
- Encrypt everything in flight

Multi-cloud security in a “Zero Trust” world

Vault

Machine Authentication & Authorization

Consul

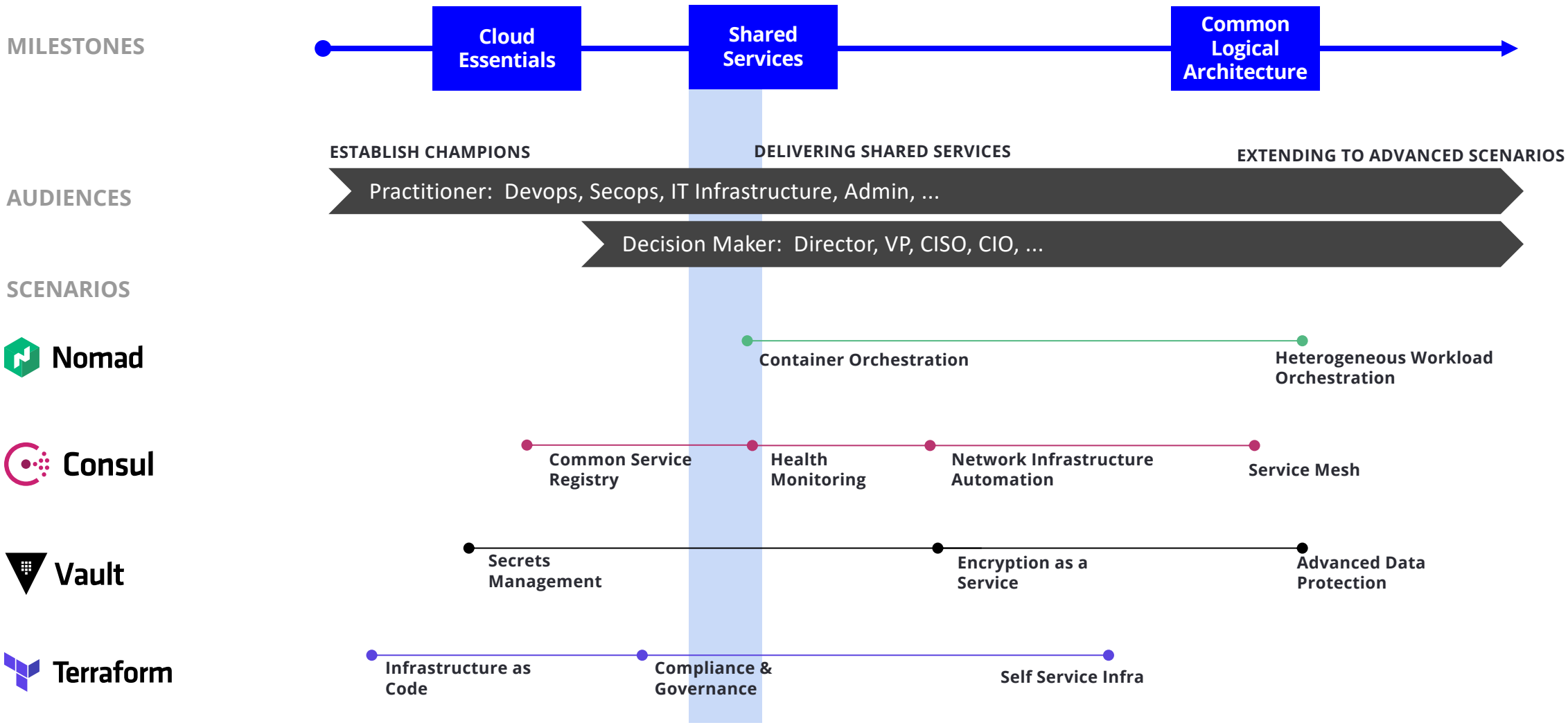
Machine-to-Machine Access

Boundary

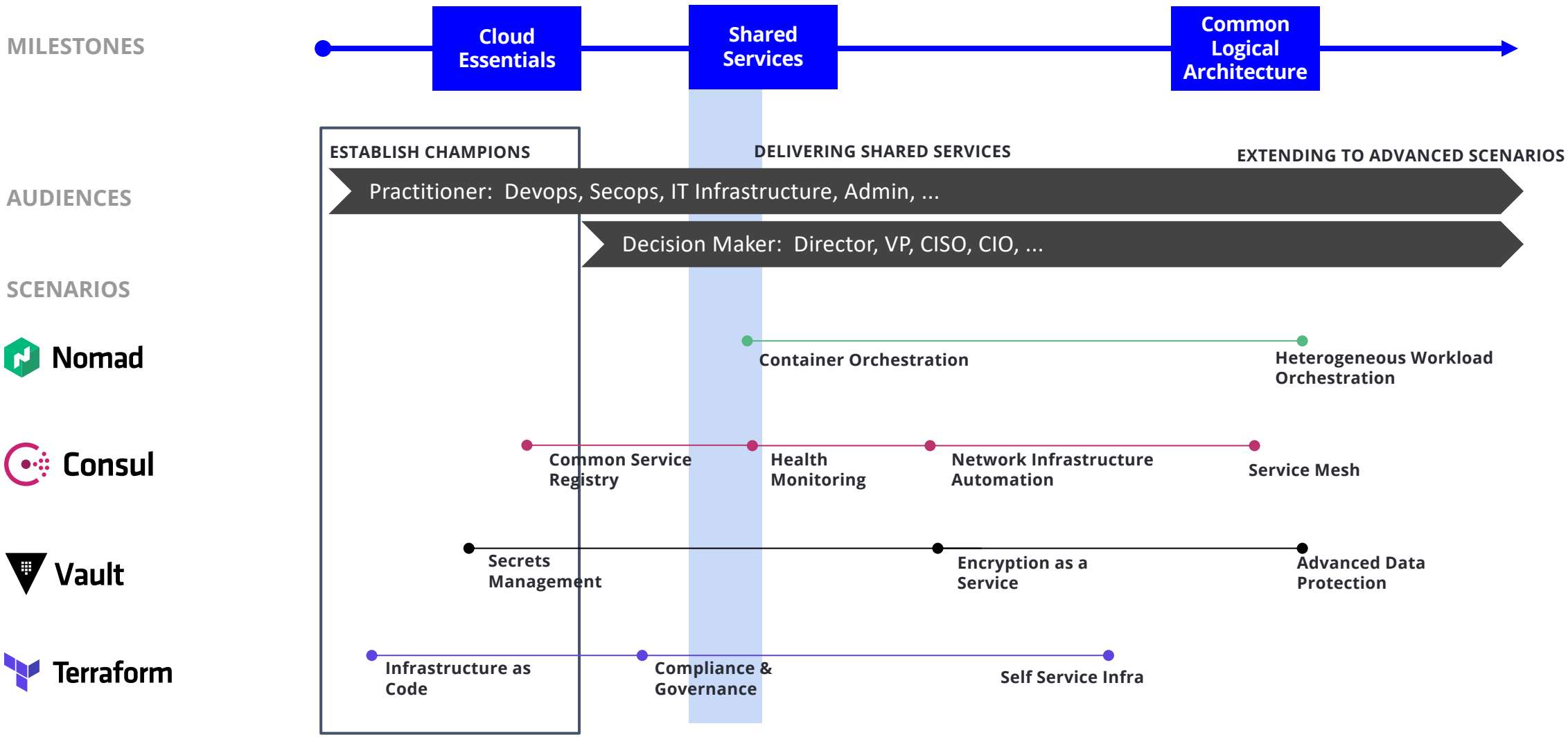
Human-to-Machine Access

Human Authentication & Authorization

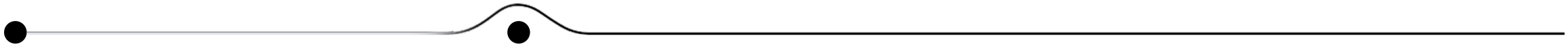
Unlocking the Customer Journey to COM



Unlocking the Customer Journey to COM



The migration to cloud security



Traditional Datacenter

Modern Datacenter

Static

Defend the Perimeter

+

Dynamic

Inoculate the Interior

=

Defense in Depth

The migration to cloud security

Traditional Datacenter

Static

Defend the Perimeter

+

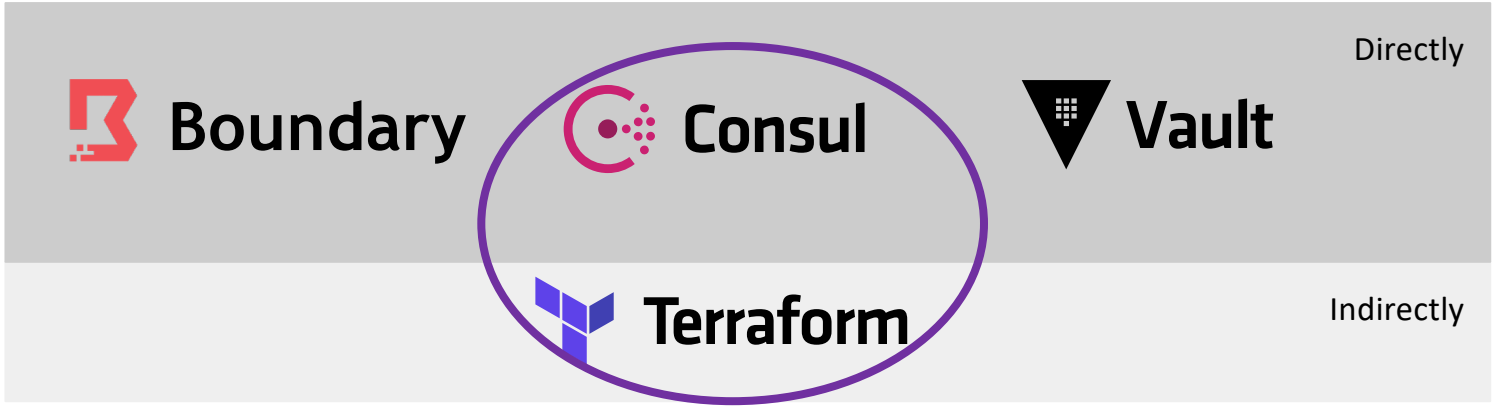
Modern Datacenter

Dynamic

Inoculate the Interior

=

Defense in Depth



IDENTITY-DRIVEN CONTROLS

CORNERSTONE CONTROLS

HashiCorp

Zero-Trust with HashiCorp

https://www.hashicorp.com/solutions/zero-trust-security

F5 & HashiCorp

SMOKE THE COMPETITION

SMOKE THE COMPETITION CHECKPOINTS

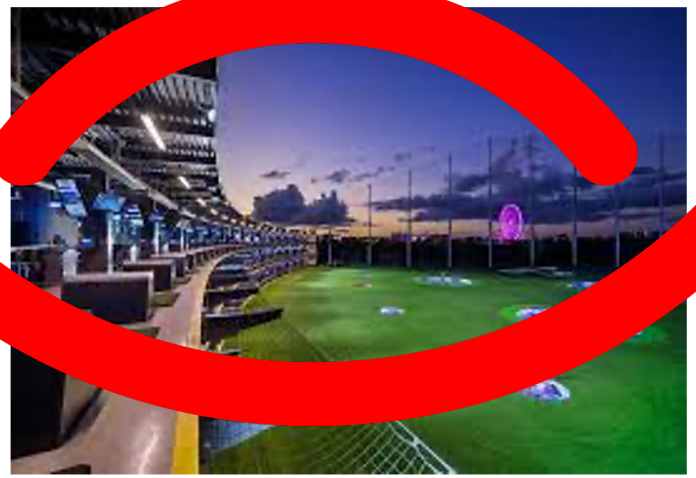
- ❑ 7/22 - Kickoff Call
- ❑ 8/12 - Mitigate OWASP Top 10
- ❑ 9/02 - NGINX KIC
- ❑ 9/23 - Bots & App Fraud
- ❑ 10/14 - Putting it all together

Complete the challenge

F5 AND HASHICORP TEC FAIRS

- ❑ Bay Ar a
- ❑ Sacram nto
- ❑ Portland

TOPGOLF



Join the fun

How to SMOKE THE COMPETITION

Activity/Task	Points Earned
Attend Checkpoint Calls	200 / Call
Complete a Task (Two per checkpoint)	100 / Task
Register PIO Opportunity by 10/18	500 / Opportunity
Close PIO Opportunity by 10/18	1,000 / Opportunity

Join the leaderboard and get paid $$$

500 Points – Register an opportunity by 10/8

$200 – Shadow a meeting to discuss opportunity

$200 – Demo a solution during the meeting

1000 Points – Book the deal by 10/8