black hat®
EUROPE 2025

Unmasking Organizations' Security Postures: Insights from Phishing-Resistant Authentication

Fei Liu
Principal Emerging Technology Researcher, Okta

The Unknown Phishing Problem

The critical blind spot in enterprise security:

What is the scope of malicious adversary-in-the-middle (AiTM) phishing user engagements?

Agenda

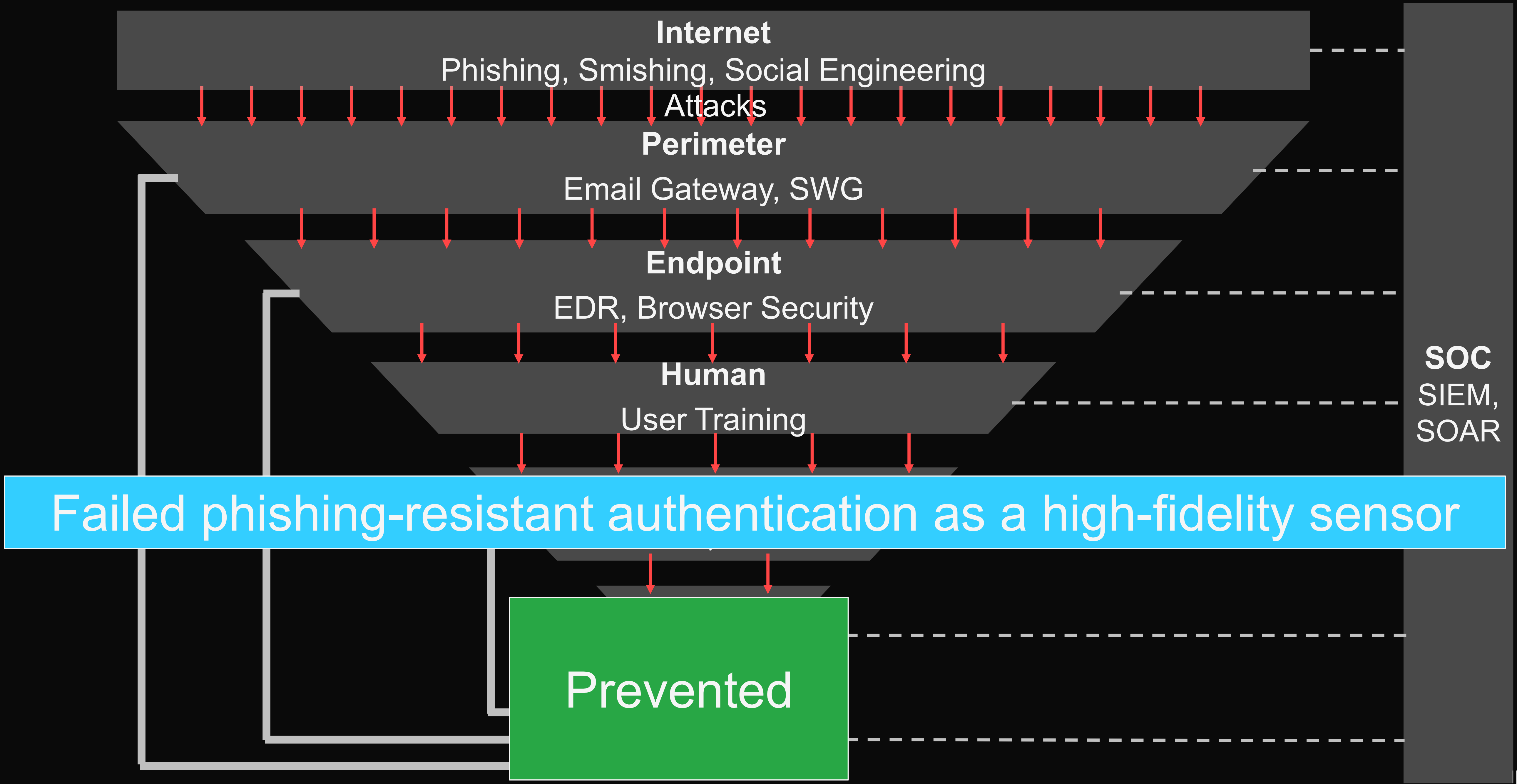
1. The Signal: A New Methodology

- How to turn failed phishing-resistant authentication into a high-fidelity sensor

An Idea

What if we could find a sensor close to account takeovers and with minimal false negatives?

A New Signal



Failed phishing-resistant authentication as a high-fidelity sensor

Phishing-Resistant Authentication

Core Principle: Origin-Binding

Legitimate Path

example.com → Authenticator →

Domain matches: 'example.com' = 'example.com’ → Login succeeds

Phishing Path

phishing.com → Authenticator →

Domain mismatches: 'phishing.com' != 'example.com’ or not exist→ Login fails

The Scale of the Study

1.5

Years Research

Thousands

Security-Mature Organizations

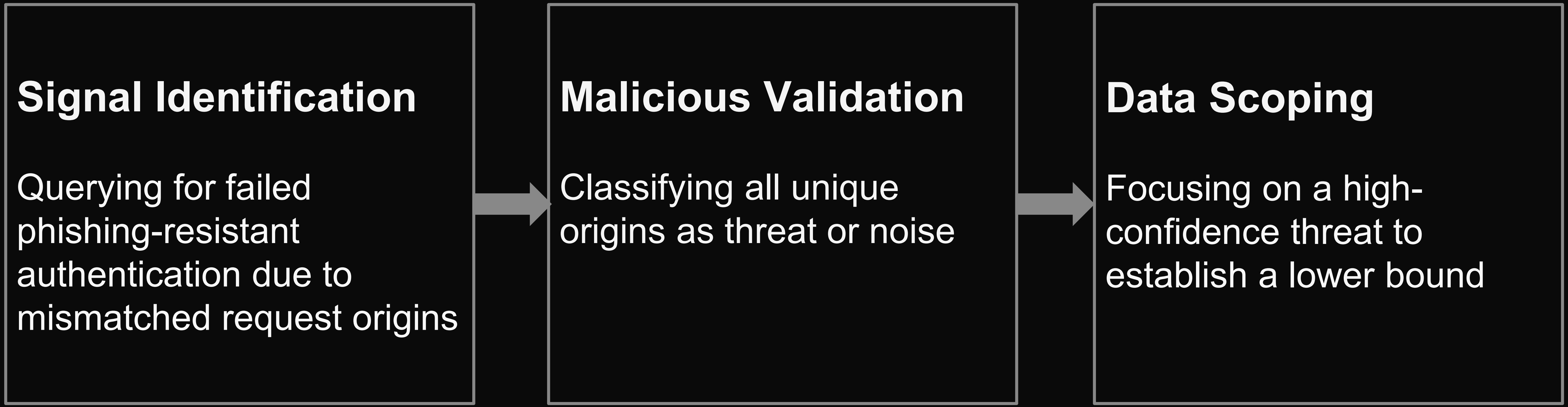
26

Months of Longitudinal Data

~3 Billion

Authentication Events Analyzed

Methodology: From Syslog to Final Dataset



Signal Identification

Querying for failed phishing-resistant authentication due to mismatched request origins

Malicious Validation

Classifying all unique origins as threat or noise

Data Scoping

Focusing on a high-confidence threat to establish a lower bound

Hunting for the Signal

Okta Syslog

Hunting Query

```
Outcome.reason eq ‘FastPass declined phishing attempt’
```

Critical Log Data

```
eventType: user.authentication.auth_via_mfa
Outcome.Reason: FastPass declined phishing attempt
Outcome.Result: FAILURE

System.DebugContext.DebugData.Risk:
{reasons=Mismatched request origin:<phishing-
domain.com>; ... Application Name: <Targeted App> ...}
```

Malicious Validation

Threat or noise? A three-pronged analysis

Expert Analysis

The internal security team categorizes origins and enriches them with threat intelligence

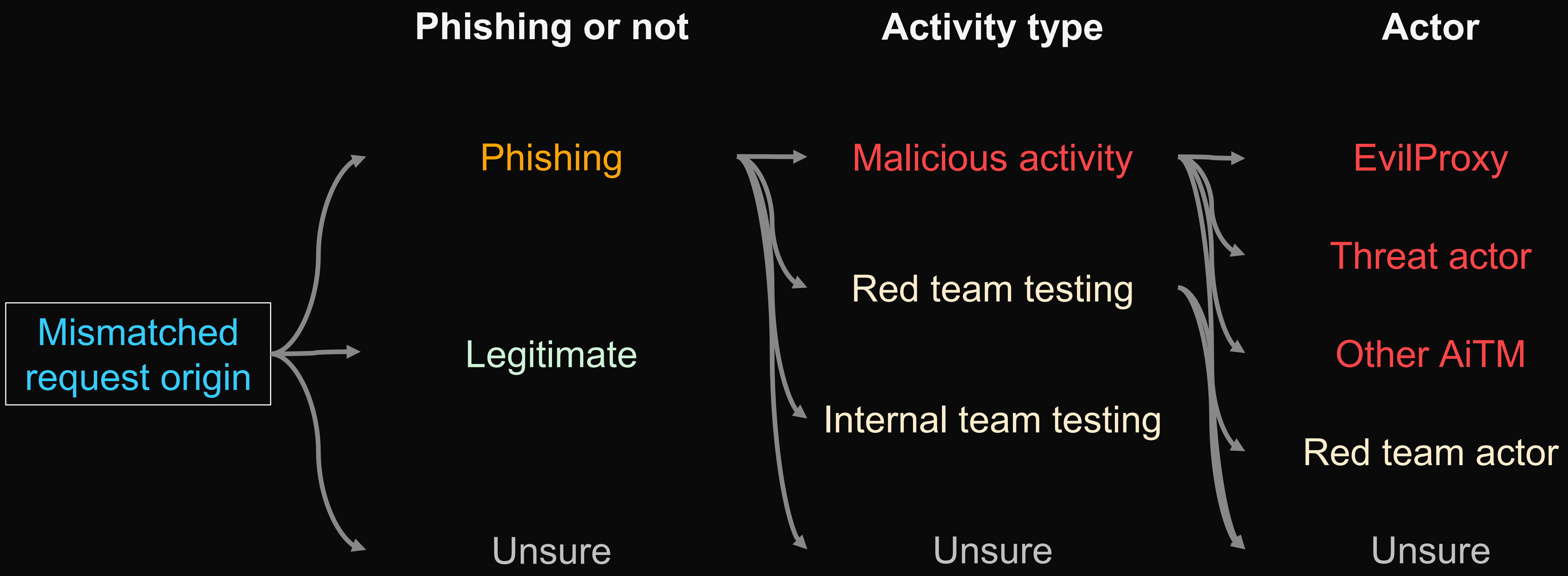
AI-Assisted Classification

An LLM, fed with threat literature, labels origins, with human verification for accuracy

Customer Validation

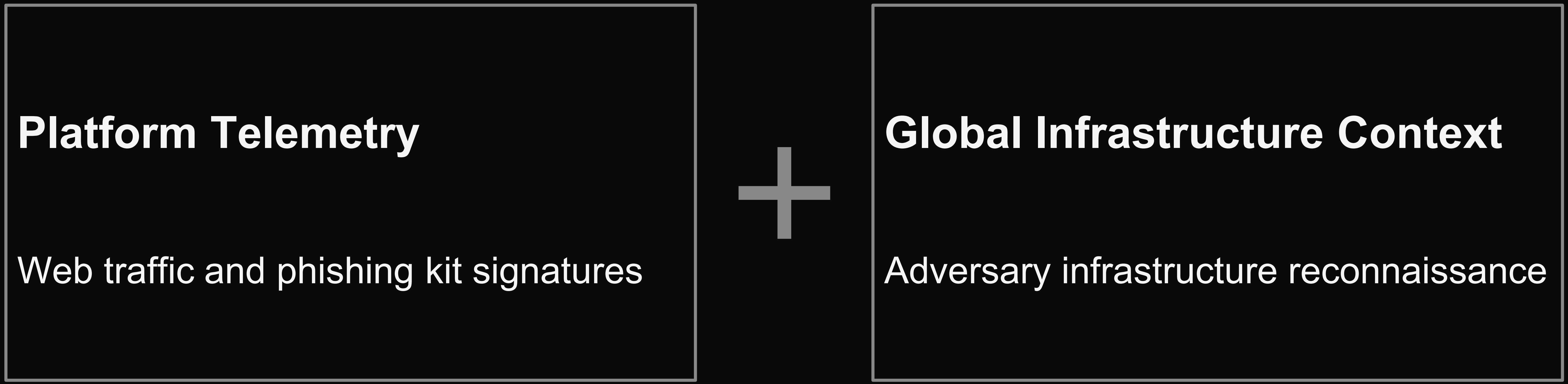
Outreach via notifications and questionnaires provides classification from customers

Hierarchical Classification Schema



Approach 1: Expert Analysis

Intelligence from cyber defense operations



Platform Telemetry

Web traffic and phishing kit signatures

Global Infrastructure Context

Adversary infrastructure reconnaissance

A high-quality initial classification

Approach 2: AI-Assisted Classification

LLM was prone to hallucination

- Provided a grounding document *
- Required reason for classification to enable rapid human verification

LLM failed on the large batch, silently dropping or combining URLs

- Manually verified all URLs by cross-referencing inputs against the LLM's final output

The LLM successfully achieved perfect alignment with expert analysis for EvilProxy classification

[* Sekoia Global analysis of Adversary-in-the-Middle phishing threats]

Approach 3: Customer Validation

Organizations

(Deep but Narrow)

+ In-depth view of their own security posture

- Only see inside their organizations
- Limited by tools and capabilities

?

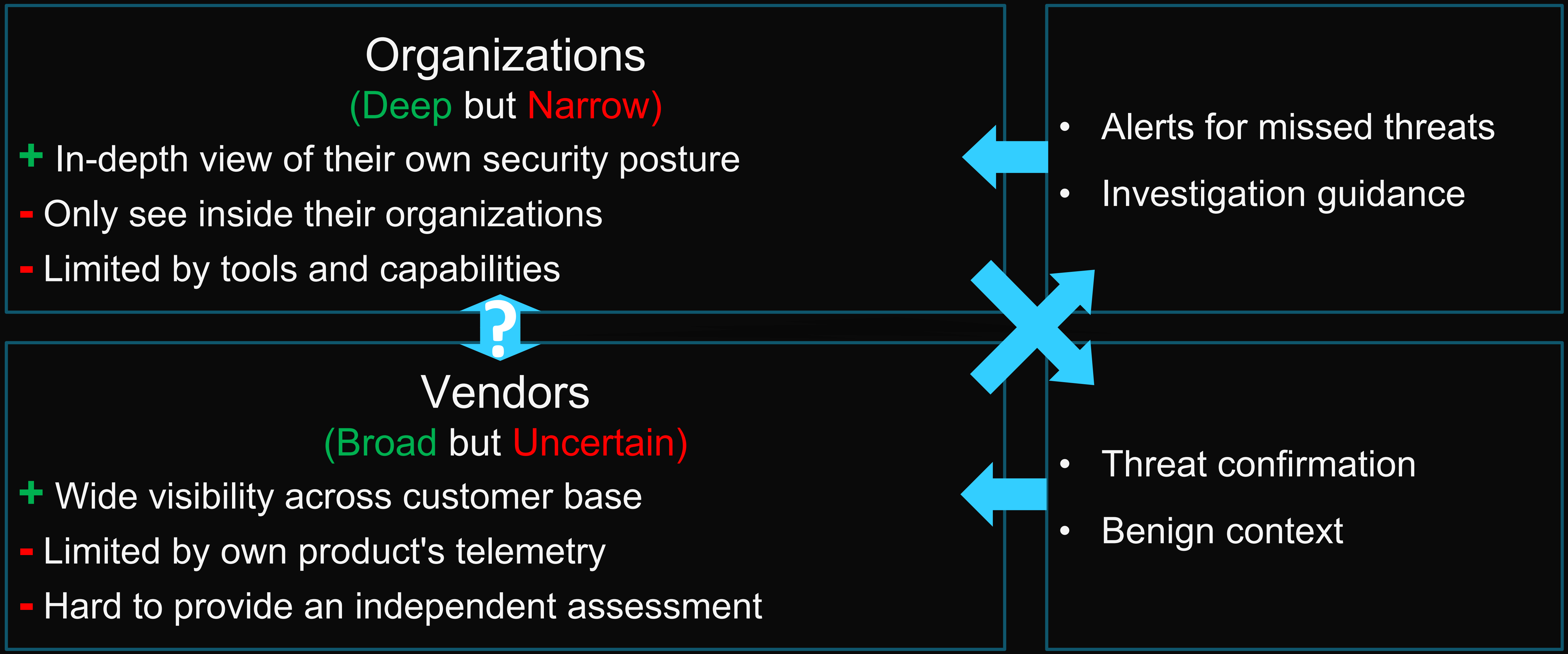
Vendors

(Broad but Uncertain)

+ Wide visibility across customer base

- Limited by own product's telemetry
- Hard to provide an independent assessment

Approach 3: Customer Validation



Organizations

(Deep but Narrow)

+ In-depth view of their own security posture

- Only see inside their organizations

- Limited by tools and capabilities

Vendors

(Broad but Uncertain)

+ Wide visibility across customer base

- Limited by own product's telemetry

- Hard to provide an independent assessment

- Alerts for missed threats
- Investigation guidance

- Threat confirmation
- Benign context

Learnings from Customer Validation

Research Win
Closing the Validation Gap

~20% response rate

- Confirmed malicious EvilProxy events
- Identified red team and internal security testing
- Understood reasons for legitimate origin domain mismatches

Learnings from Customer Validation

Research Win
Closing the Validation Gap

~20% response rate

- Confirmed malicious EvilProxy events
- Identified red team and internal security testing
- Understood reasons for legitimate origin domain mismatches

Security Win
Closing the Awareness Gap

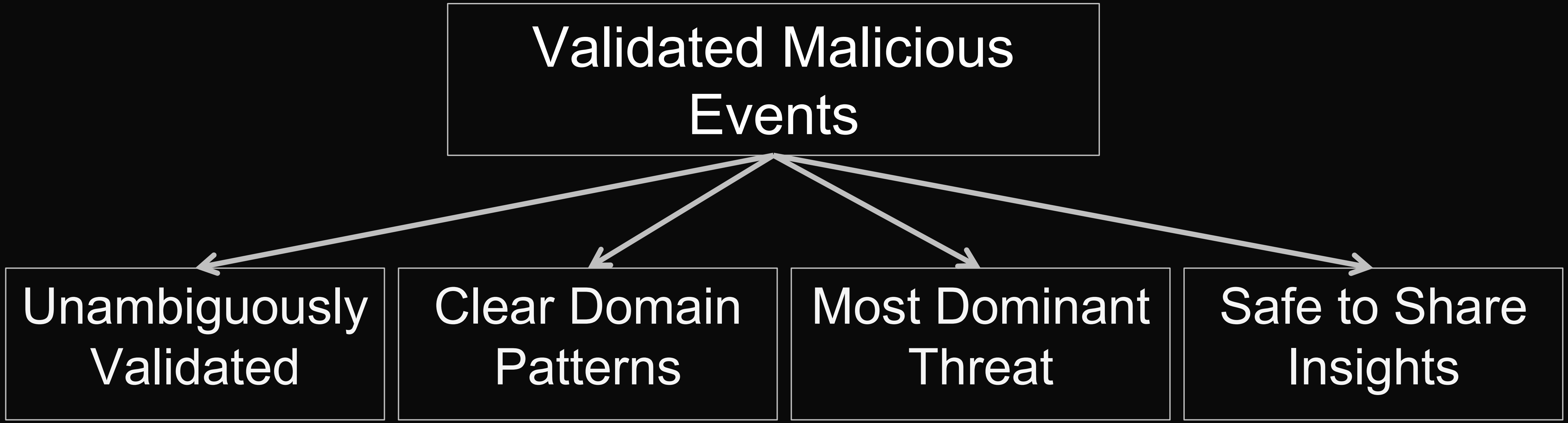
5 of 7 EvilProxy incidents

- Admins reported they had not detected them until our notification
- Admins suggested using the signal for incident response, SIEM enhancement, and IP blocking

An ongoing feedback loop (active for 9 months)

Scope the Dataset

Establishing a conservative lower bound



Validated Malicious Events

Unambiguously Validated

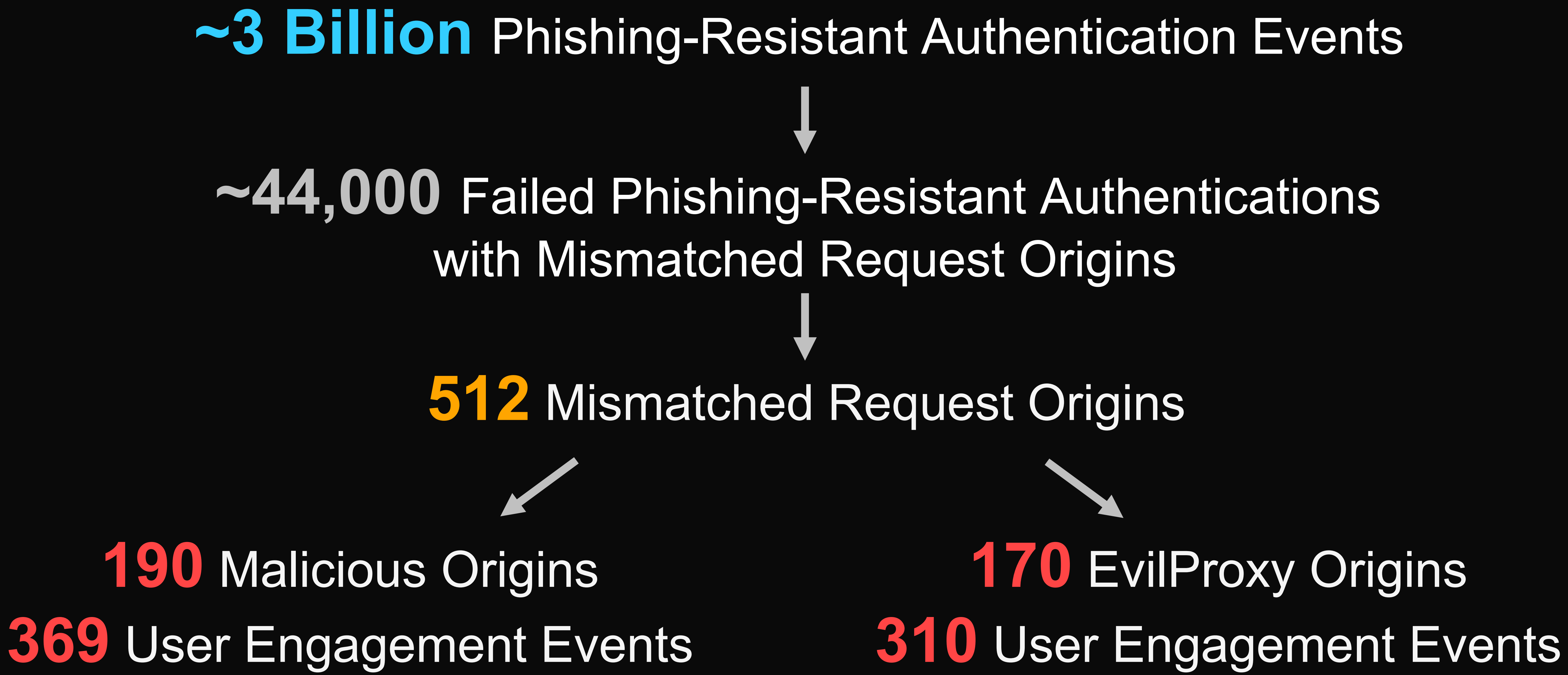
Clear Domain Patterns

Most Dominant Threat

Safe to Share Insights

The lower-bound dataset: ***EvilProxy campaigns***

Validated Dataset



~3 Billion Phishing-Resistant Authentication Events

~44,000 Failed Phishing-Resistant Authentications with Mismatched Request Origins

512 Mismatched Request Origins

190 Malicious Origins
369 User Engagement Events

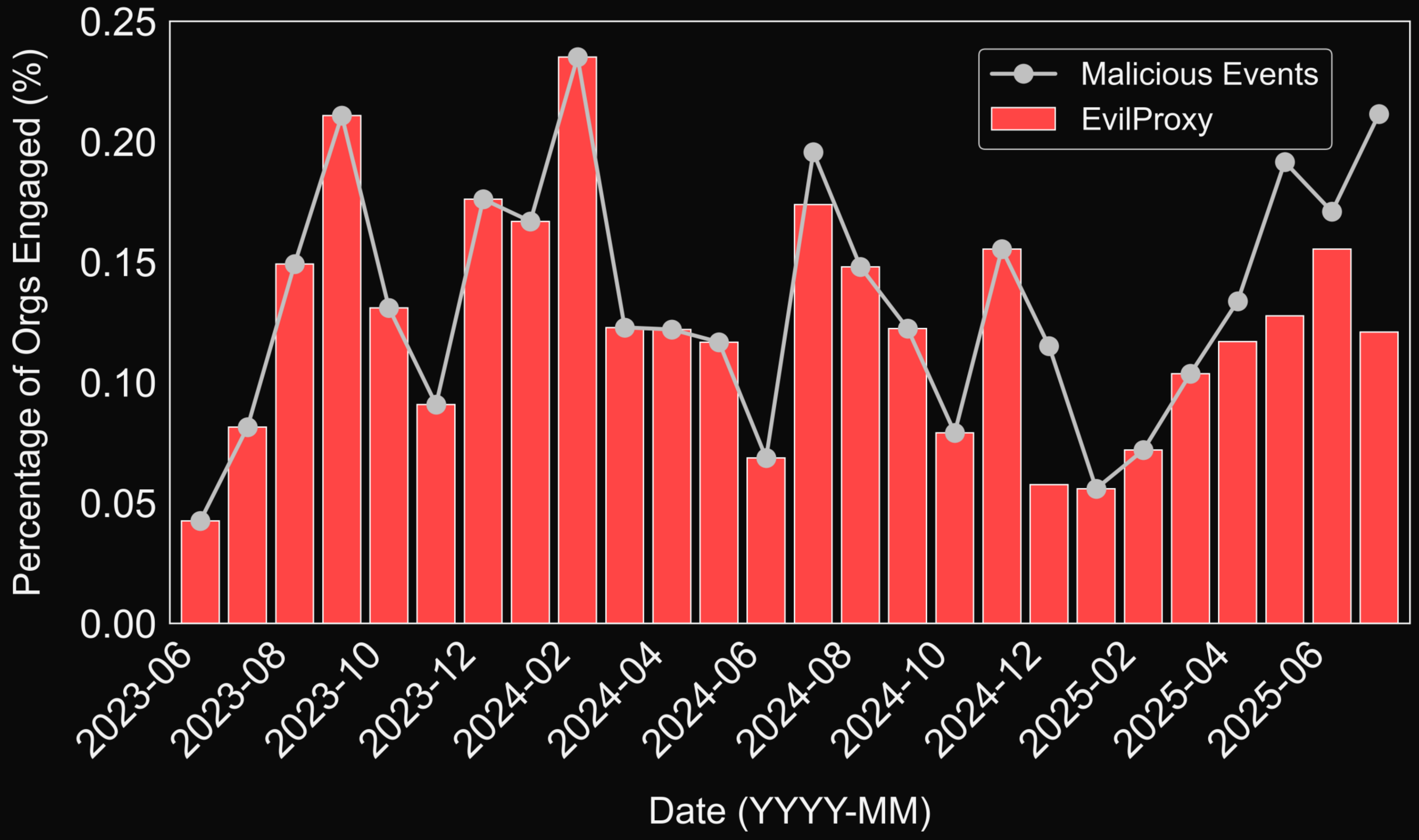
170 EvilProxy Origins
310 User Engagement Events

Agenda

1. The Signal: A New Methodology
   - How to turn failed phishing-resistant authentication into a high-fidelity sensor

2. The Evidence: Empirical Insights
   - What two years of malicious AiTM phishing reveals about enterprise threats

AiTM Phishing Threat is Persistent



What Did the Attackers Actually Do

Infrastructure: leveraging commercial cloud

- Top 10 ISPs in the syslog were cloud/VPS providers
  1. Akamai Connected Cloud (Linode)
  2. DigitalOcean

Authentication phishing domains: disposable

- Attackers used rapid rotation to evade blocklists, some had more engagments, e.g. kanakratna[.]com

Phishing kits: old still works

- Older EvilProxy kit responsible for more user engagements

Who was Being Successfully Engaged

Geography: Americas-focused

- Organizations in Americas were engaged more than in EMEA and APAC

Organization size: all sizes, but a higher rate for larger ones

- Largest enterprises (20,000+) were most frequently engaged

Industry: broad industry coverage

- Professional Services organizations were engaged at the highest rates

Application: O365 was the overwhelming lure

- Successful engagements were largely redirected from Microsoft O365

Agenda

1. The Signal: A New Methodology
   - How to turn failed phishing-resistant authentication into a high-fidelity sensor
2. The Evidence: Empirical Insights
   - What two years of malicious AiTM phishing reveals about enterprise threats
3. The Implications: Defense in Precision
   - How to apply these findings to your security practice

Lower-Bound Estimate

0.12%/Month

0%/Month

of organizations that have malicious AiTM phishing user engagements

Lower-Bound Estimate

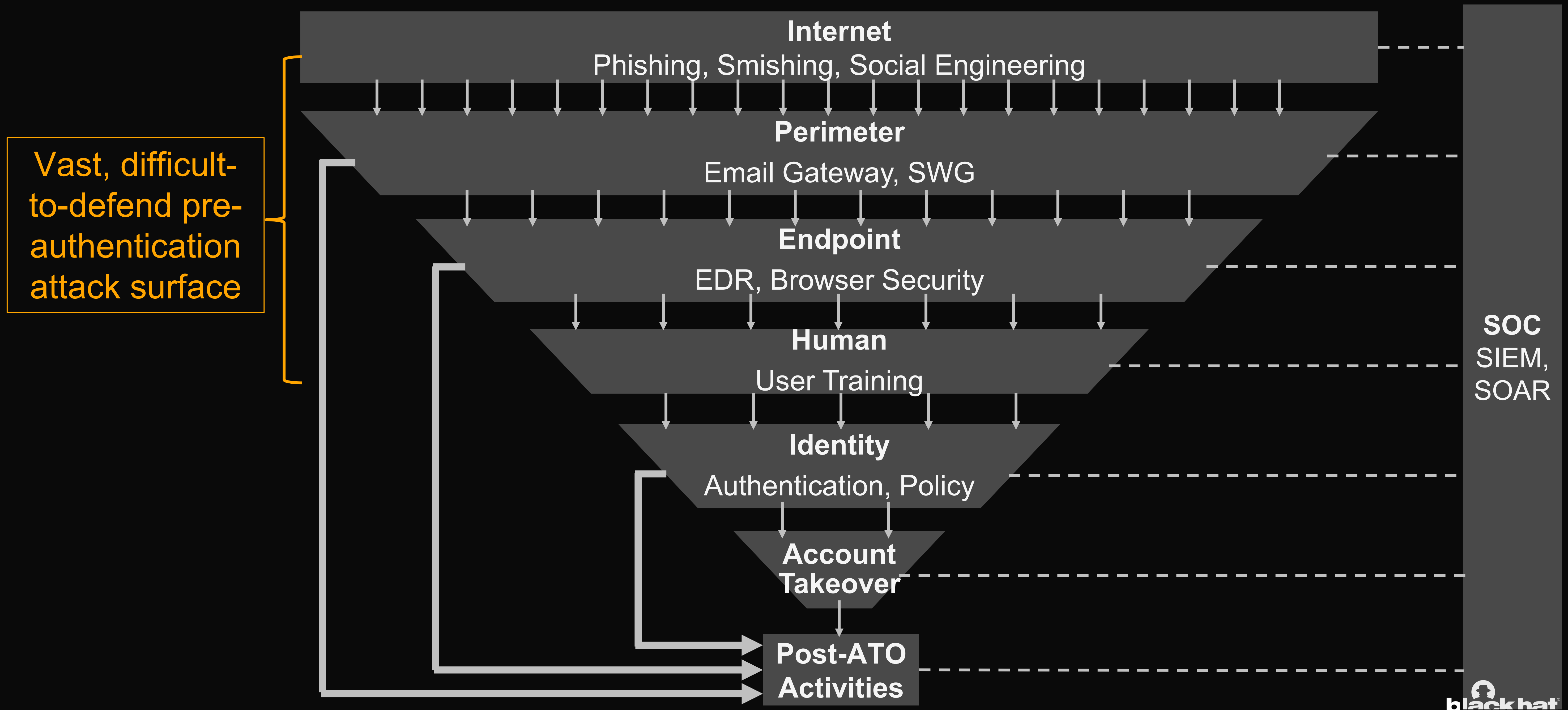
0.12% /Month

of organizations that have malicious AiTM phishing user engagements

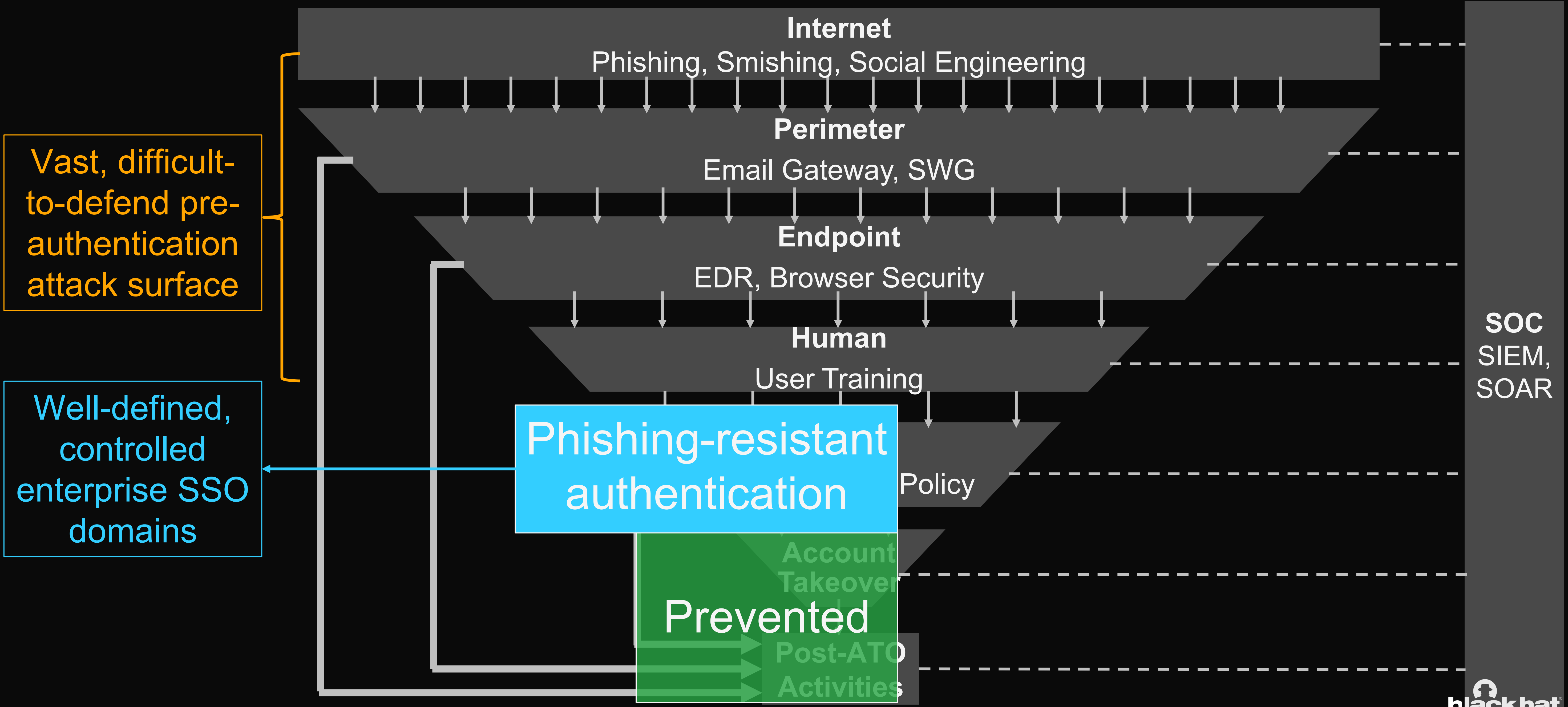
This number is intentionally conservative

- Strict conservatism in threat inclusion criteria
- An overestimation of the total number of protected organizations
- A bias toward security-mature organizations

Defense in Precision



Defense in Precision



Internet
Phishing, Smishing, Social Engineering
Perimeter
Email Gateway, SWG
Endpoint
EDR, Browser Security
Human
User Training
Policy
Account Takeover
Post-ATO Activities
SOC
SIEM, SOAR
Vast, difficult-to-defend pre-authentication attack surface
Well-defined, controlled enterprise SSO domains
Phishing-resistant authentication
Prevented

The Complete Picture

Attacker Reality

- AiTM PhaaS for just $400/month *
- Broad target coverage with low effort
- Repeatable success

* Resecurity EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web

The Complete Picture

Attacker Reality

- AiTM PhaaS for just $400/month *
- Broad target coverage with low effort
- Repeatable success

Defender Reality

- Pre-Authentication defenses insufficient
- MFA not fully adopted (70% **), and ineffective
- Phishing-resistant MFA adoption gaining momentum (14% **)

* Resecurity EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web

** Okta Secure Sign-in Trends Report 2025

The Complete Picture

Attacker Reality

- AiTM PhaaS for just $400/month *
- Broad target coverage with low effort
- Repeatable success

Defender Reality

- Pre-Authentication defenses insufficient
- MFA not fully adopted (70% **), and ineffective
- Phishing-resistant MFA adoption gaining momentum (14% **)

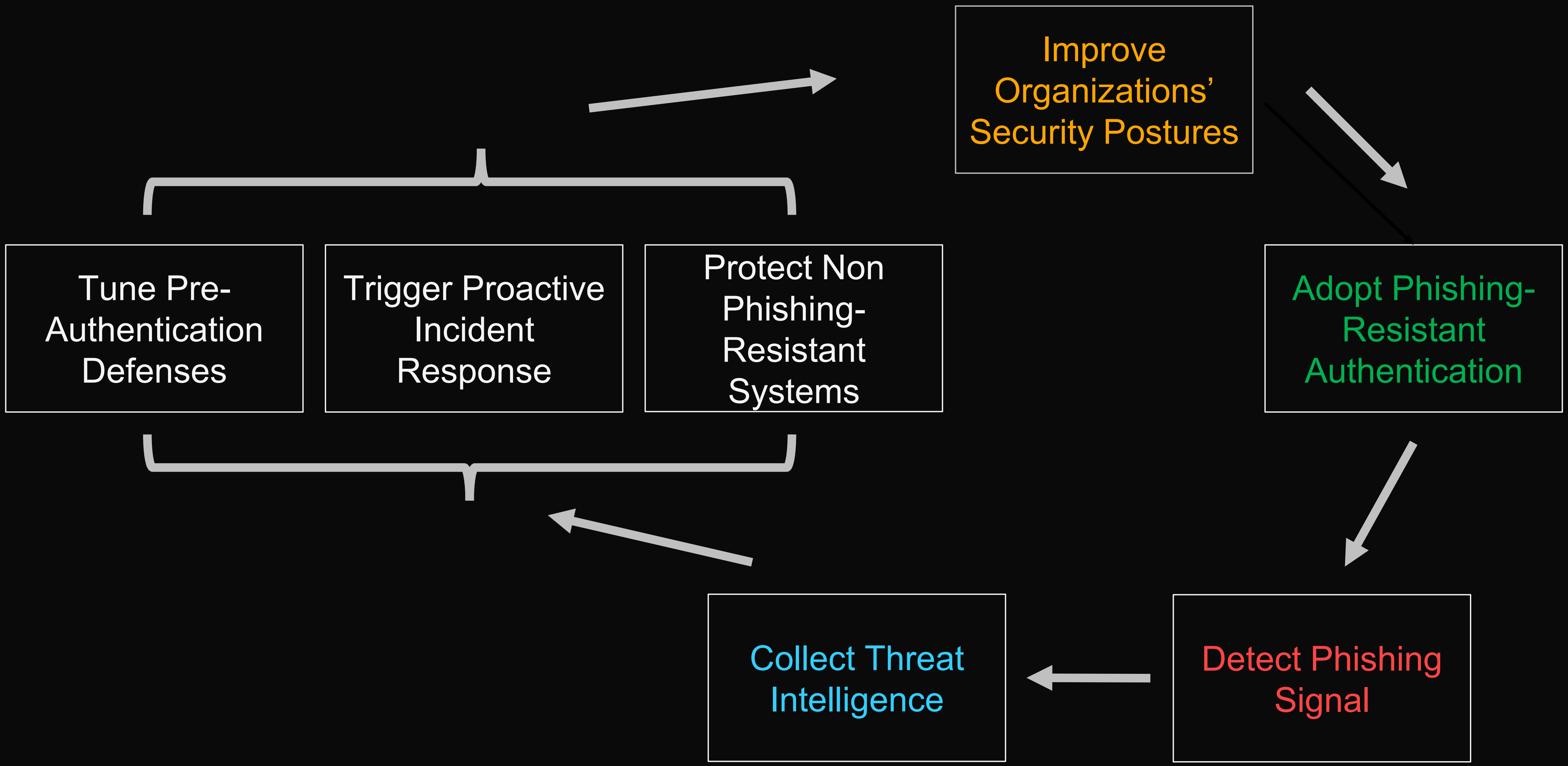
Defender Ideal

- Block the phishing attempt (shield)
- Identify the threat (sensor)
- Minimize identity-based phishing

* Resecurity EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web

** Okta Secure Sign-in Trends Report 2025

Hope: A Sensor That Grows with Adoption



Improve Organizations' Security Postures

Adopt Phishing-Resistant Authentication

Detect Phishing Signal

Collect Threat Intelligence

Tune Pre-Authentication Defenses

Trigger Proactive Incident Response

Protect Non Phishing-Resistant Systems

Agenda

1. The Signal: A New Methodology
   - How to turn failed phishing-resistant authentication into a high-fidelity sensor

2. The Evidence: Empirical Insights
   - What two years of malicious AiTM phishing reveals about enterprise threats

3. The Implications: Defense in Precision
   - How to apply these findings to your security practice

4. The Playbook: Sound Bytes and Call to Action
   - What you need to do next to enhance your organization’s security posture

Sound Bytes

Your true phishing risk may be higher than you think.

- Sophisticated attacks constantly exploit security gaps and user vulnerabilities.

Your current posture may have a blind spot.

- Pre-authentication controls are insufficient, also need strong authentication.

Phishing-resistant authentication is both a shield and a sensor.

- Prevent phishing but also provide timely and high-fidelity detection.

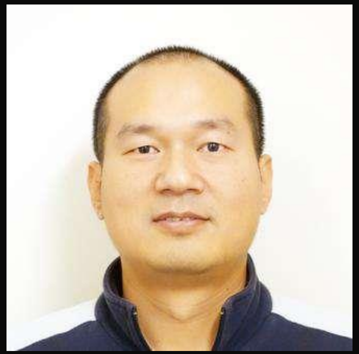
Call to Action

Enterprise security postures are insufficient.

Prioritize phishing-resistant authentication
and integrate high-fidelity alerts
to respond to phishing attacks you could miss.

It has been a Team Sport

Moussa Diallo



Yu Liu

Gabriel Marusic

Gary Khemani

Kelly Kern

Justin Bergez

Erik Kuhrman

Angie Yanez

Dave Case

Matt Egan

Karim Lalji

Justin Boots

THANK YOU

Get the full research & demo

Fei Liu

fei.liu@okta.com

linkedin.com/in/fei-liu-pt/