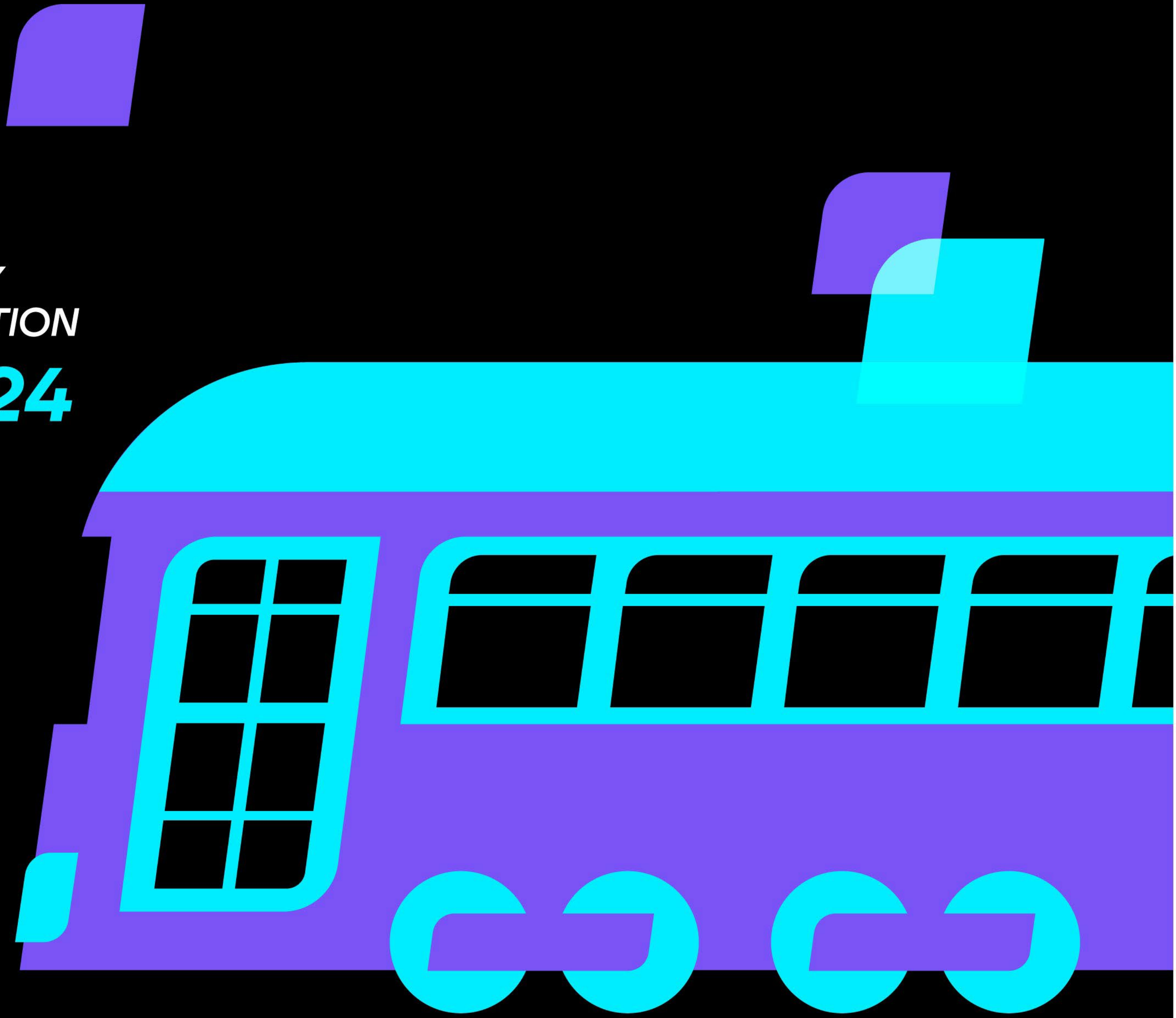
HYBRID
IDENTITY
PROTECTION

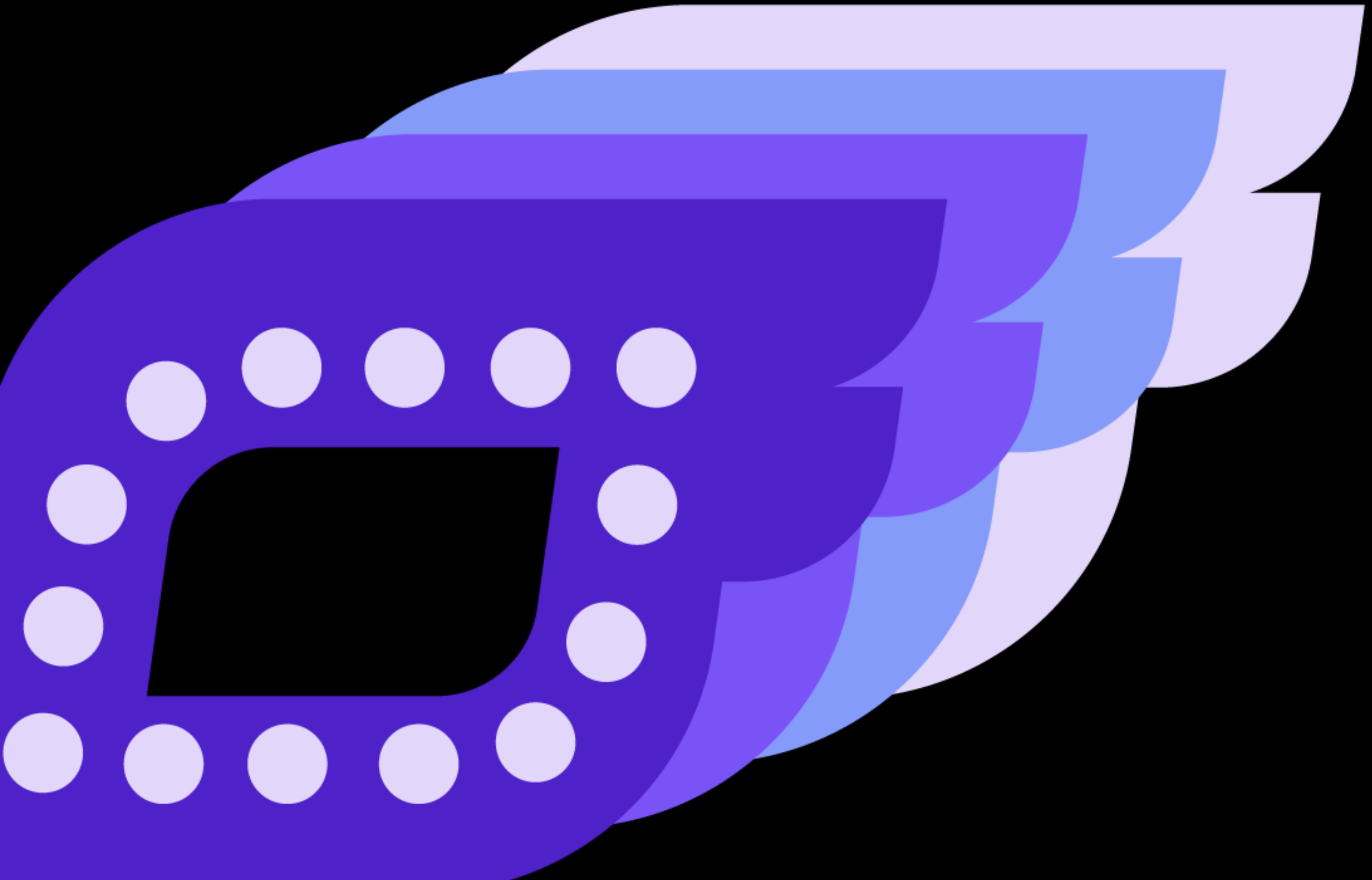
conf24

# NEW ORLEANS



HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS



# The Oak and the Willow

Alexander Weinert

VP Identity Security, Microsoft

# Introductions

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

## Alexander Weinert

VP Identity Security, Microsoft

Alex is the VP of Identity Security at Microsoft. Billions of users sign into millions of apps every day on our identity platforms; the Identity Security team protects them from unauthorized access, account takeover, and abuse.

Co-presented by two ancient warriors, two trees, and Sean Deuby.

# Sun Tzu

Minister, Helu of Wu (500 BCE)

Sun Tzu was a Chinese military general, strategist, philosopher, and author of The Art of War, an influential work that has affected both Western and East Asian philosophy and military thought. Sun Tzu is revered in Chinese and East Asian culture as a legendary historical and military figure.

https://en.wikipedia.org/wiki/Sun_Tzu

# Miyamoto Musashi

Sword Saint of Japan (1640 CE)

Miyamoto was a Japanese swordsman, strategist, artist, and writer who became renowned through stories of his unique double-bladed swordsmanship and undefeated record in his 62 duels. He was the founder of the Niten Ichi-ryū style of swordsmanship, and in his final years authored The Book of Five Rings

https://en.wikipedia.org/wiki/Miyamoto_Musashi

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

# The Oak

## Hardwood Tree, Earth

An oak is a hardwood tree or shrub in the genus Quercus of the beech family. They have spirally arranged leaves, often with lobed edges, and a nut called an acorn, borne within a cup. The genus is widely distributed in the Northern Hemisphere; it includes some 500 species, both deciduous and evergreen. Fossil oaks date back to the Middle Eocene.

https://flic.kr/p/21ZAvX6
https://en.wikipedia.org/wiki/oak

# The Willow

## Deciduous Tree, Earth

Willows, of the genus Salix, comprise typically deciduous trees and shrubs. Willows all have abundant watery bark sap, soft, usually pliant, tough wood, slender branches, and large, fibrous roots. The roots are remarkable for their toughness, size, and tenacity to live, and roots readily sprout from aerial parts of the plant.

https://en.wikipedia.org/wiki/Willow

# Hard Style (Oak) and Soft Style

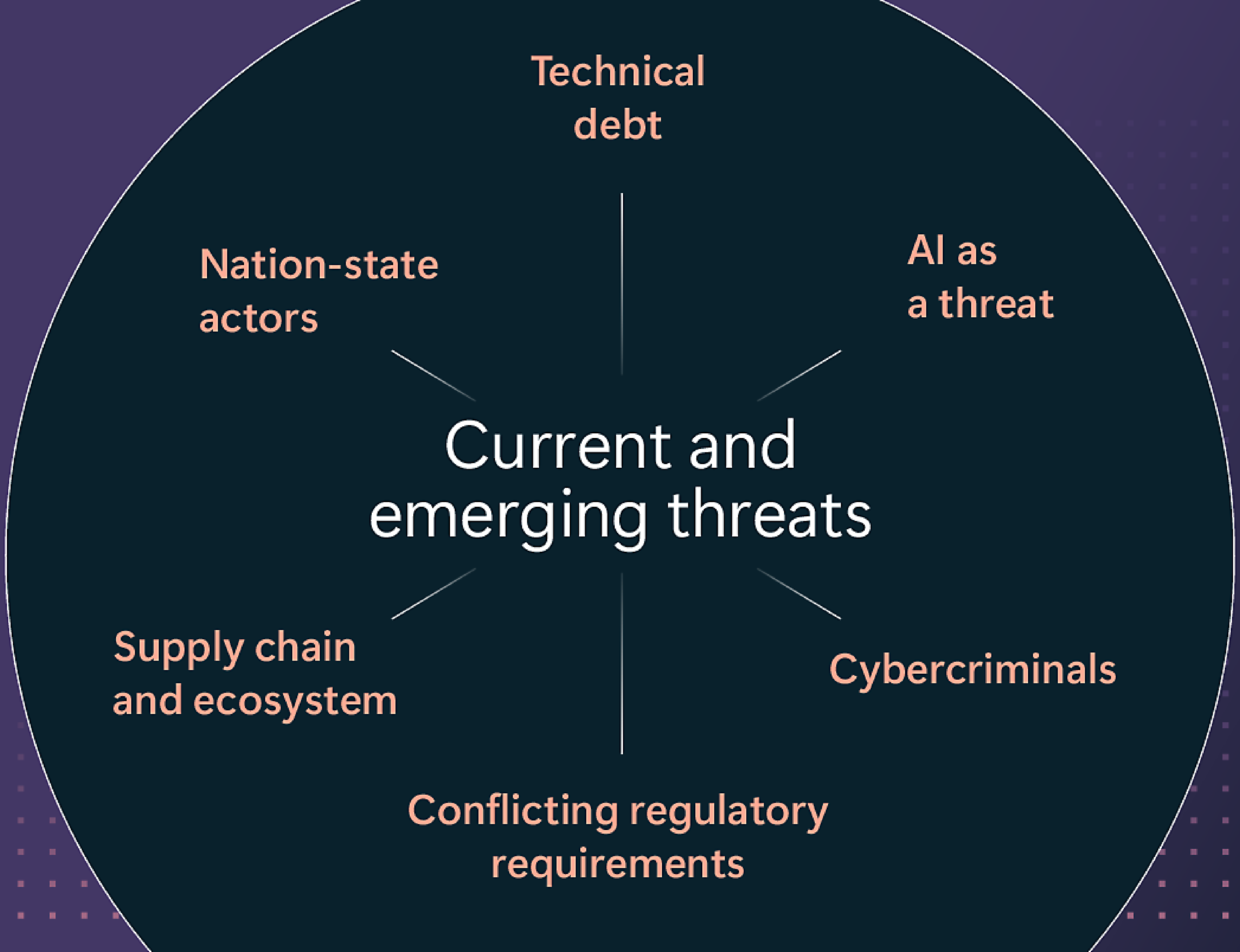
- Hard Style:
  - Closed fist
  - Linear movement
  - Rigid stance
  - Best against soft targets
- Soft Style:
  - Open hand
  - Circular moment
  - Fluid stance
  - Best against hard targets

**Alex Weinert (in ’92)**

Chinese Kempo 1990-2010

**Sean Deuby (in ‘04)**

Shorin-Ryu, 1979-2020



Current and emerging threats

Technical debt

AI as a threat

Cybercriminals

Conflicting regulatory requirements

Supply chain and ecosystem

Nation-state actors

# Trends in 2024

## Proliferation of identities

**>300B**

passwords in use by humans and machines

## Employees access more than

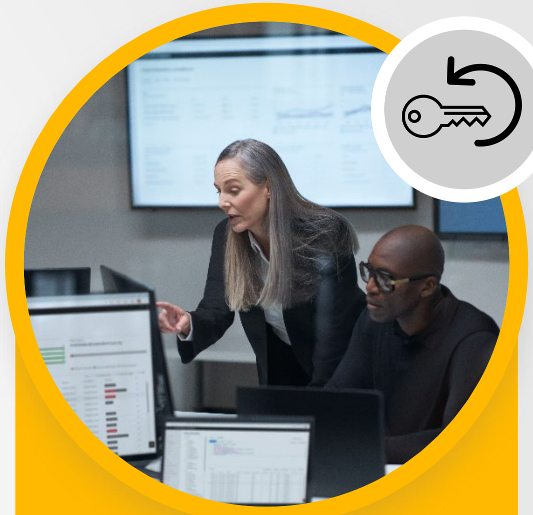
**1,500**

applications in the average enterprise

## Increase in cybercrime

**4,000**

password attacks per second in 2023



## Token Replay attacks

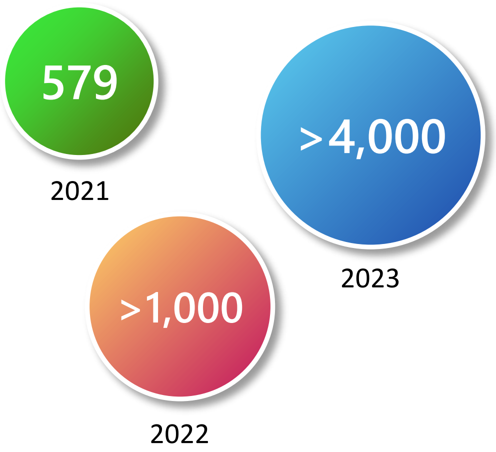
**2x**

increase since 2023

Cybersecurity Statistics and Trends - 2024 & Beyond (Cybersecurity for me)
Microsoft Zero Trust deployment guide for your applications
Microsoft Digital Defense Report 2023 (MDDR)
How to break the token theft cyber attack chain (2024 Microsoft blog)

# The odds are against defenders

Password attacks per second



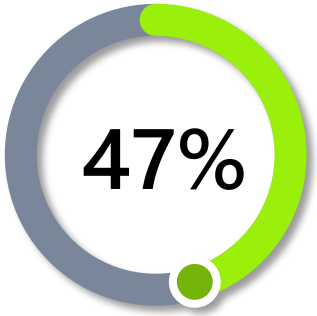
Source: Microsoft

Organizations use an average of 80 security tools

80

Source: Microsoft

Increase in phishing attacks, driven by attacker use of AI

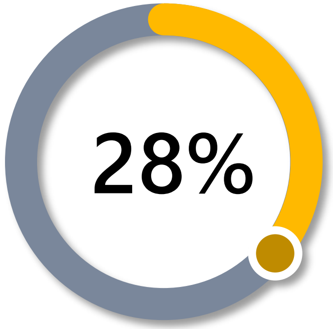


Source: Zscaler

Open cybersecurity jobs globally

4M

Source: (ISC)2



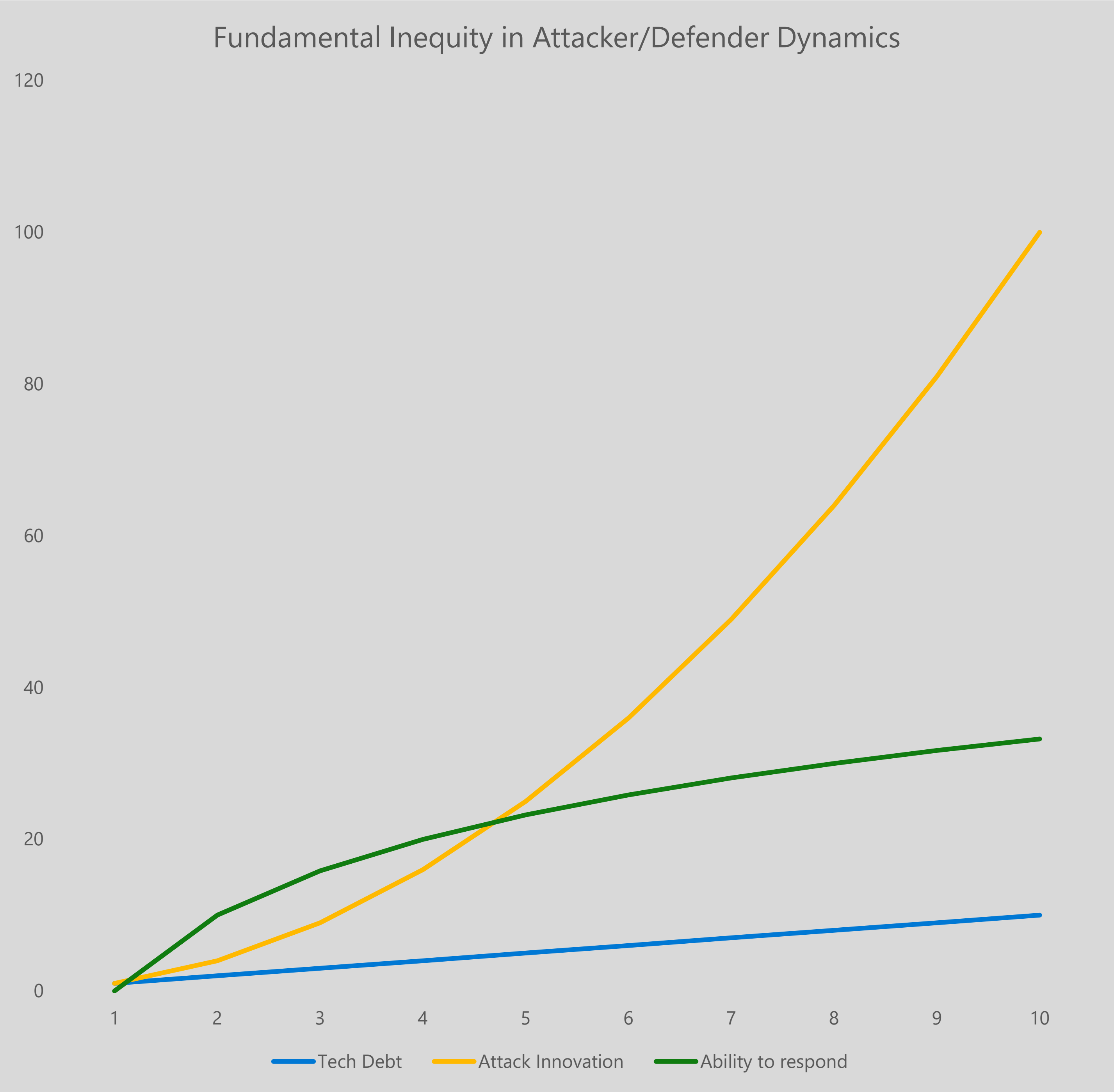
Business leaders concerned about data or IP loss due to improper use of AI

Source: IDC

# A stacked deck

Technical Debt adds surface area for attackers and slows response capabilities for defenders.

Threats are evolving much faster than the tech you care for.

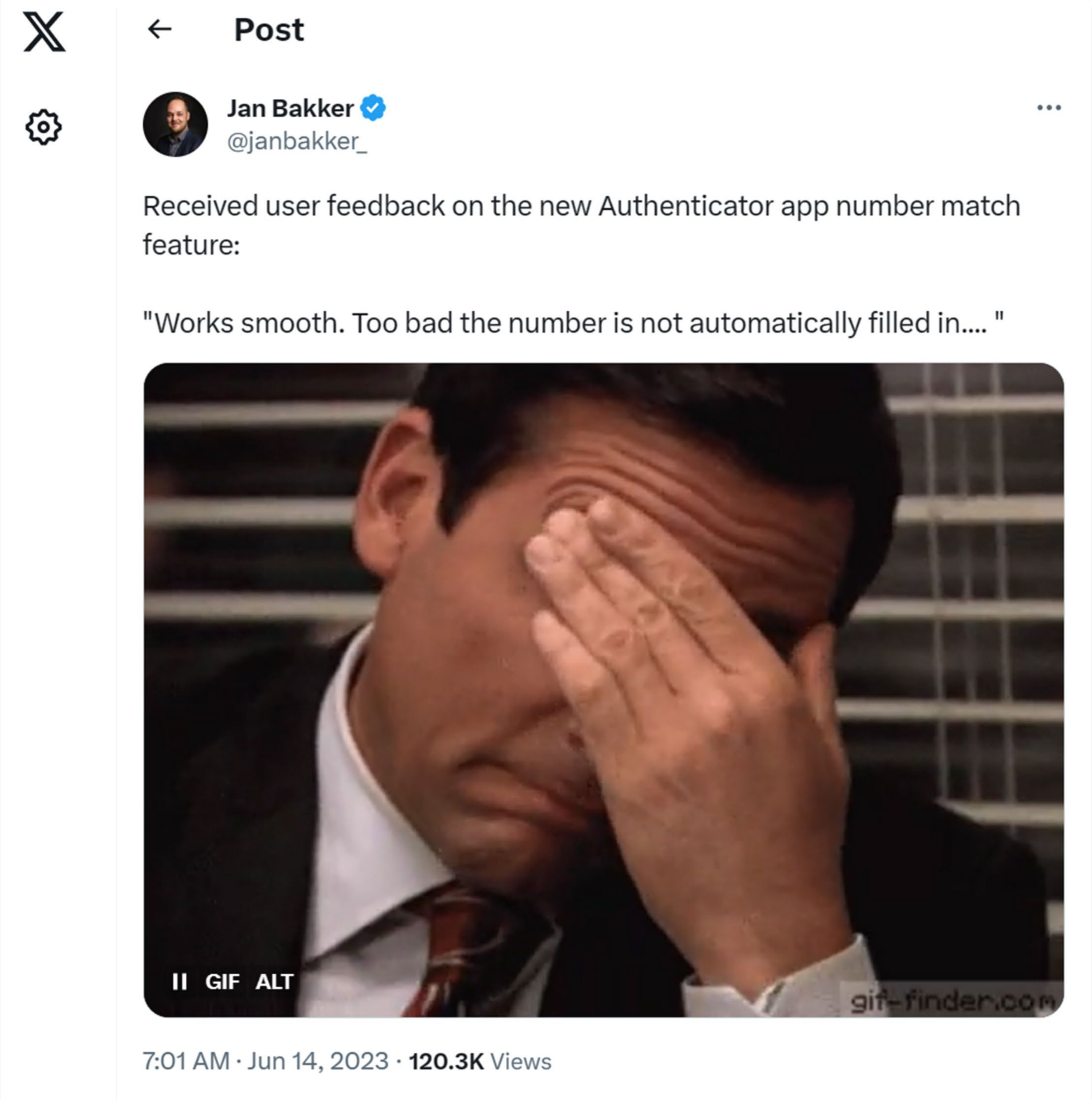


# Ungovernable Users

Users can not be trained to deal with these attacks.

High frequency of user failure overwhelms SOC resources

Strategy: Make flows failure-proof



Jan Bakker
@janbakker_

Received user feedback on the new Authenticator app number match feature:

"Works smooth. Too bad the number is not automatically filled in.... "

7:01 AM · Jun 14, 2023 · 120.3K Views

# Workload identities need to be secured

## Lack of management for workload identities and their permissions leaves sensitive data vulnerable

**~70%**

of workload identities have access to sensitive data

**>80%**

of workload identities are inactive

**<5%**

of access permissions assigned to workload identities are used

Source: 2023 State of Cloud Permissions Risks report

“It is better to be a warrior in a garden, than a gardener in a war.”
– Miyamoto Musashi

# How to talk to gardeners

- Show business impact of vulnerabilities
- Show business benefits of defenses
- This requires accounting we often don’t have

- Anecdote: Xbox
  - Determine drop off rate post compromise and lost revenue
  - Determine chargebacks resulting from compromise
  - Determine cost of support
  - Show cost savings (COGS impact) of

“Do nothing that is of no use”
– Miyamoto Musashi

# Scarce Resources Require Hard Decisions

- E.g.
  - Incrementally improve password spray detection?
  - Incrementally reduce SMS fraud?
  - Invest in anti-phish training?
  - Apply PW filter?

    …
  - Move everyone to passkey?

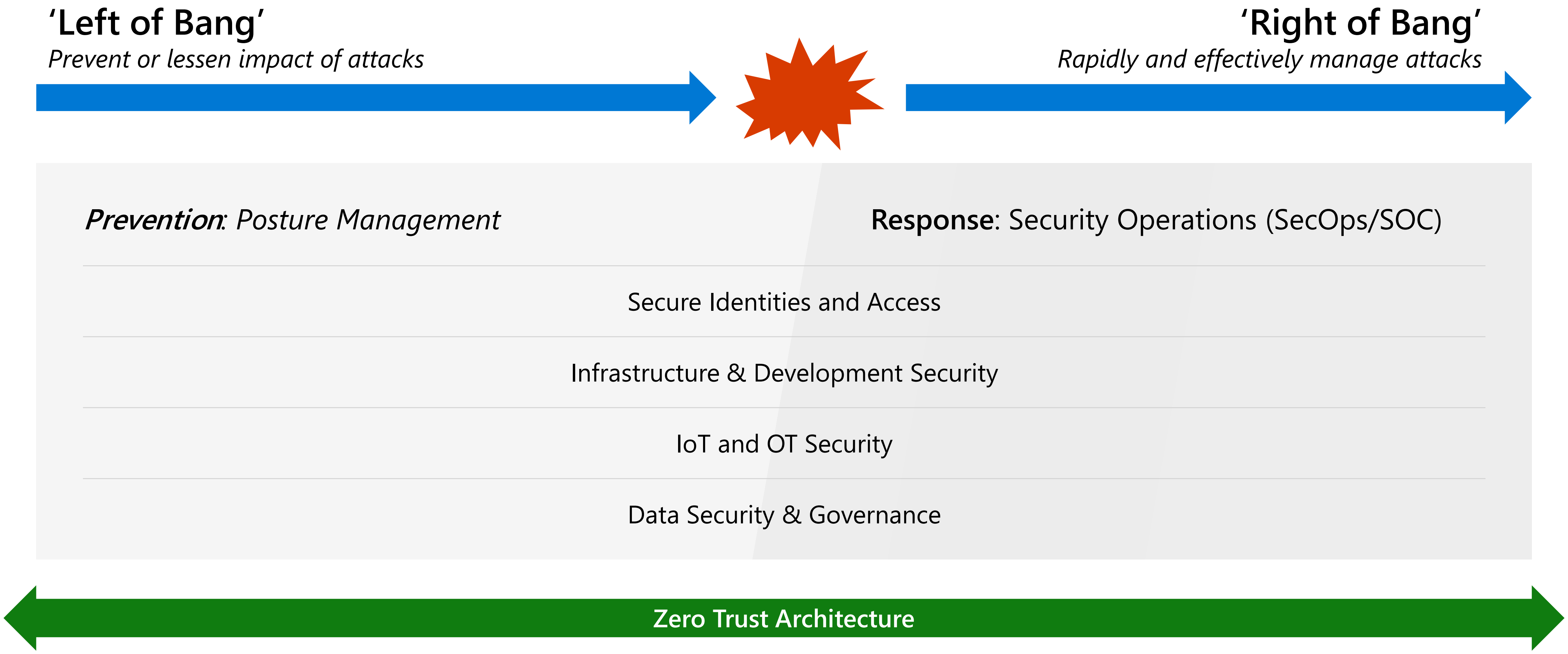
# “Sweat more during peace, bleed less during war.”
# - Sun Tzu

HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS

# Security is Complex

Must cover entire technology estate across the security lifecycle and prioritize by business risk



**‘Left of Bang’**

*Prevent or lessen impact of attacks*

**‘Right of Bang’**

*Rapidly and effectively manage attacks*

***Prevention***: *Posture Management*

**Response**: Security Operations (SecOps/SOC)

Secure Identities and Access

Infrastructure & Development Security

IoT and OT Security

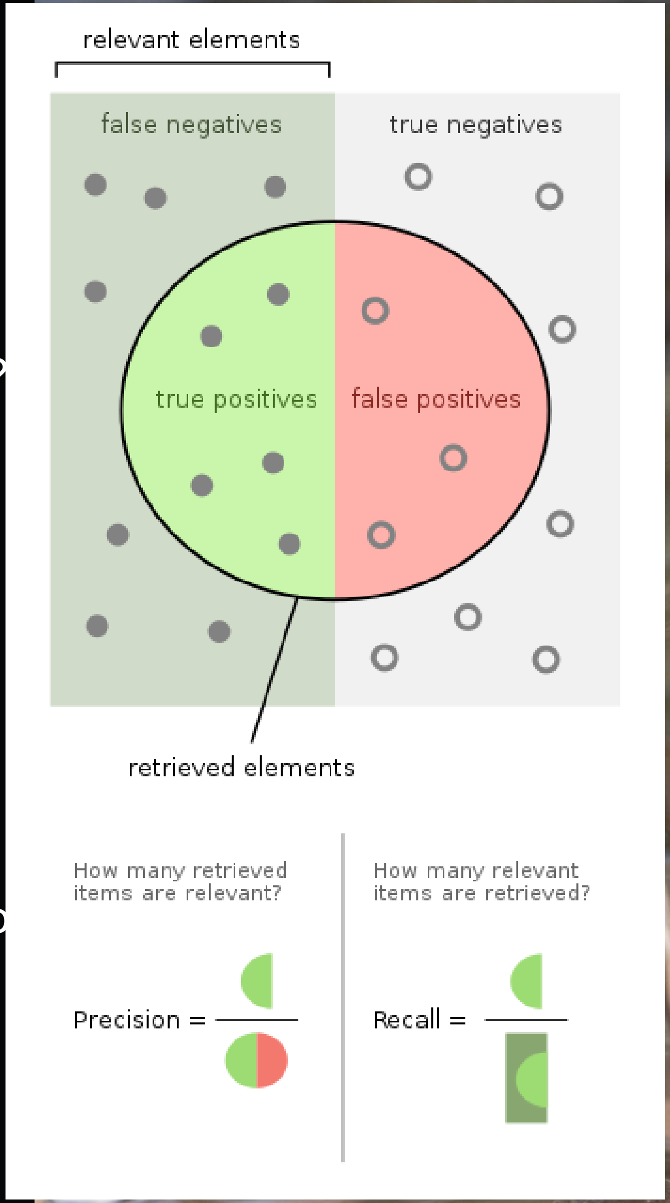
Data Security & Governance

**Zero Trust Architecture**

“To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.”
- Sun Tzu

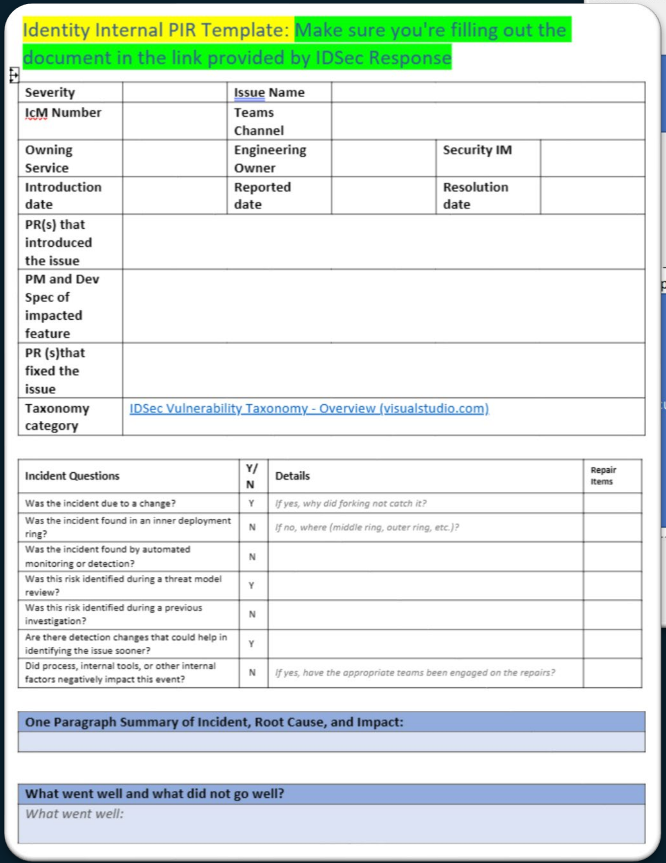
# Precision and Friction

- Precision: % of detections that are true+?
- Recall: % of attacks we caught?
- Precision & recall have inverse relations
- Overwhelmed SOCs demand highest precision signals – meaning a lot of attacks are missed.
- These create huge downstream costs.
- Your goal:
- impose LOW friction at LOW precision
- impose HIGH friction at HIGH precision
- Shift load from SOC to general populatio



“You must learn the spirit of crushing as if with a hand-grip.” - MM

# Intentional Change Management



Identity Internal PIR Template: Make sure you're filling out the document in the link provided by IDSec Response

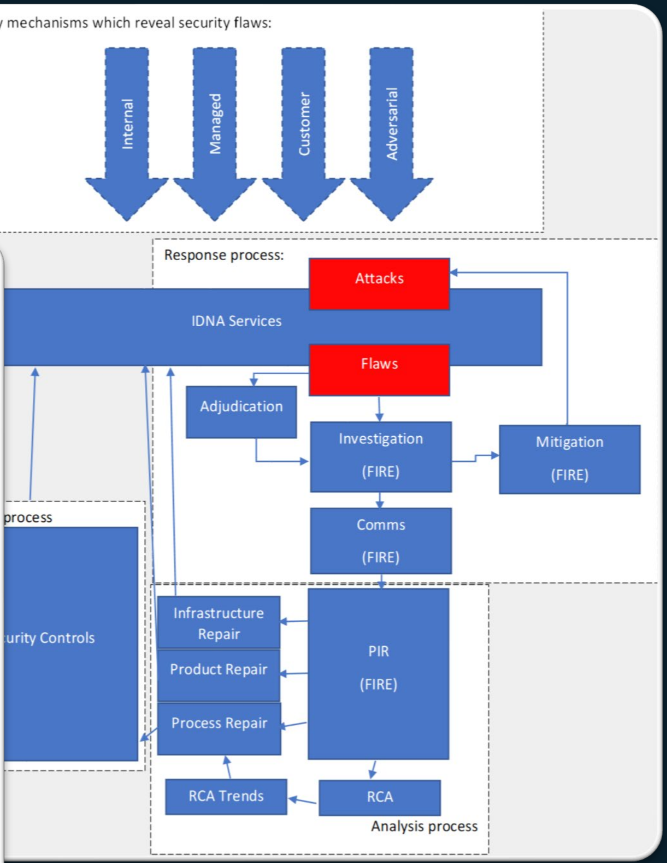
| | | | | | |
|---|---|---|---|---|---|
| **Severity** | | **Issue Name** | | | |
| **IcM Number** | | **Teams Channel** | | | |
| **Owning Service** | | **Engineering Owner** | | **Security IM** | |
| **Introduction date** | | **Reported date** | | **Resolution date** | |
| **PR(s) that introduced the issue** | | | | | |
| **PM and Dev Spec of impacted feature** | | | | | |
| **PR (s)that fixed the issue** | | | | | |
| **Taxonomy category** | IDSec Vulnerability Taxonomy - Overview (visualstudio.com) | | | | |

| **Incident Questions** | **Y/ N** | **Details** | **Repair Items** |
|---|---|---|---|
| Was the incident due to a change? | Y | *If yes, why did forking not catch it?* | |
| Was the incident found in an inner deployment ring? | N | *If no, where (middle ring, outer ring, etc.)?* | |
| Was the incident found by automated monitoring or detection? | N | | |
| Was this risk identified during a threat model review? | Y | | |
| Was this risk identified during a previous investigation? | N | | |
| Are there detection changes that could help in identifying the issue sooner? | Y | | |
| Did process, internal tools, or other internal factors negatively impact this event? | N | *If yes, have the appropriate teams been engaged on the repairs?* | |

**One Paragraph Summary of Incident, Root Cause, and Impact:**

**What went well and what did not go well?**

*What went well:*



Discovery mechanisms which reveal security flaws:

Internal

Managed

Customer

Adversarial

Response process:

Attacks

IDNA Services

Flaws

Adjudication

Investigation (FIRE)

Mitigation (FIRE)

Comms (FIRE)

process

urity Controls

Infrastructure Repair

Product Repair

Process Repair

PIR (FIRE)

RCA Trends

RCA

Analysis process

“Know your enemy, know his sword.”
- Miyamoto Musashi

# We're **defenders building defenses**

**Analyzing**

65T

threat signals every day

**Protecting**

+70B

identity and email threats blocked

**Partnering**

15K

partners in our security ecosystem

**Protecting**

860K

organizations in 120 countries

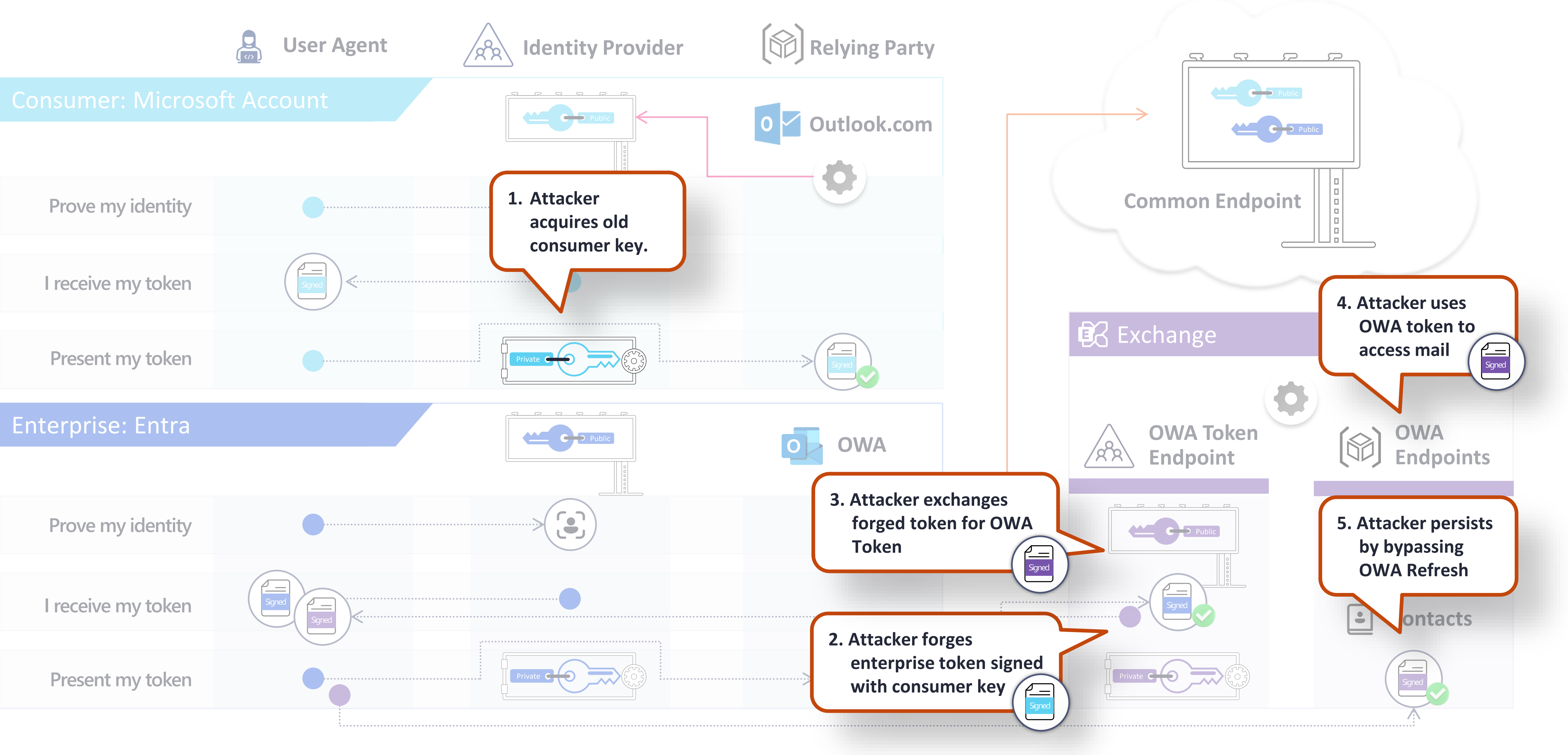
**Protecting**

10K

security professionals

“If you do not control the enemy, the enemy will control you”
– Miyamoto Musashi

# June 2023 - Storm-0558 attack mechanics



1. Attacker acquires old consumer key.

2. Attacker forges enterprise token signed with consumer key

3. Attacker exchanges forged token for OWA Token

4. Attacker uses OWA token to access mail

5. Attacker persists by bypassing OWA Refresh

# Midnight Blizzard Jan 2024

- Midnight blizzard gains access to Microsoft email

"Get beyond love and grief: exist for the good of Man."
– Miyamoto Musashi

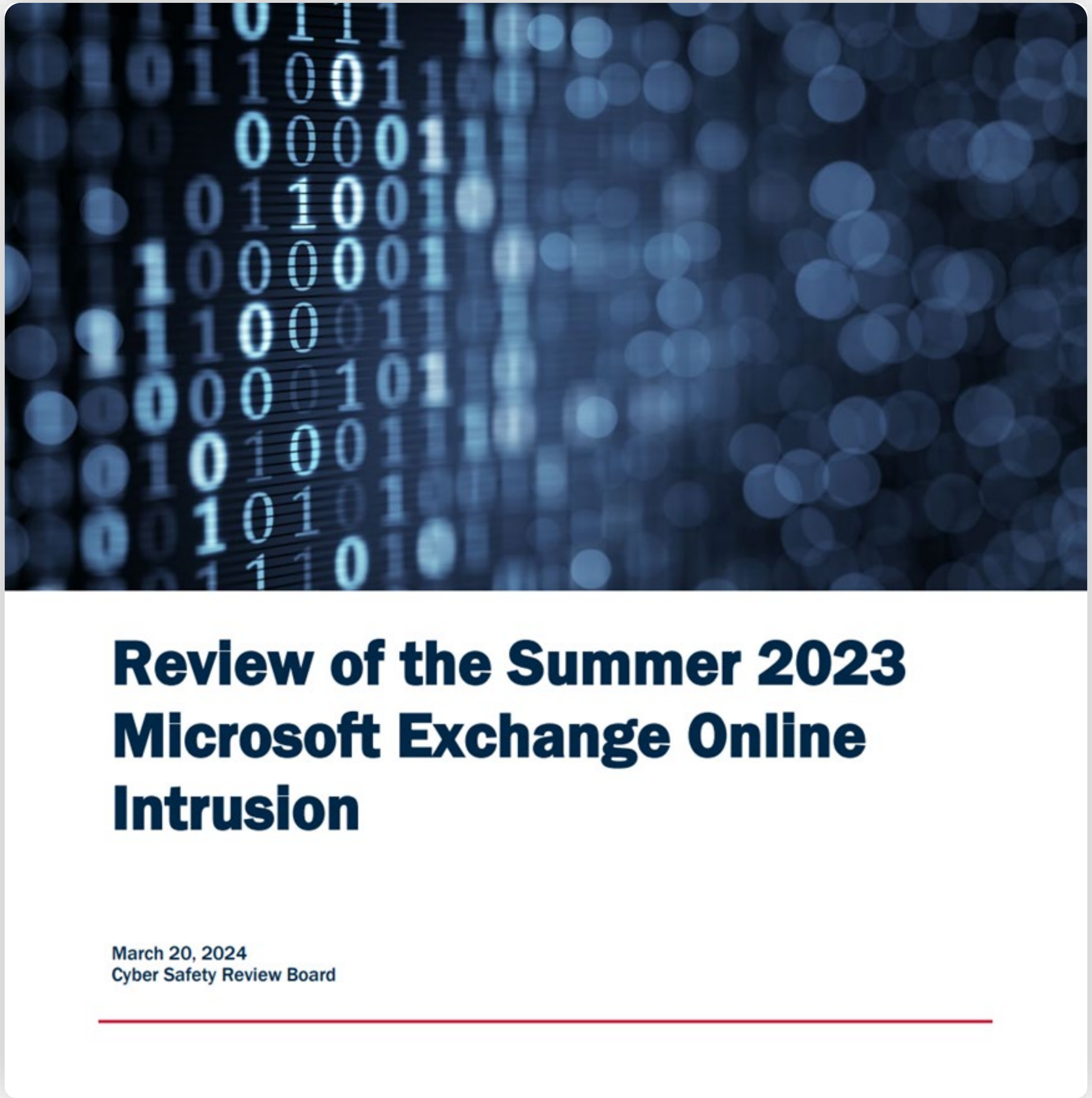
# Growth Mindset

The recent findings by the Department of Homeland Security's Cyber Safety Review Board (CSRB) regarding the Storm-0558 cyberattack from last July, and the Midnight Blizzard attack we reported in January, underscore the severity of the threats facing our company and our customers.

Microsoft plays a central role in the world's digital ecosystem, and this comes with a critical responsibility to earn and maintain trust. **We must and will do more.**

We are **making security our top priority at Microsoft, above all else**—over all other features. We're expanding the scope of SFI, integrating the recent recommendations from the CSRB as well as our learnings from Midnight Blizzard to ensure that our cybersecurity approach remains robust and adaptive to the evolving threat landscape.

aka.ms/SFIblog



Review of the Summer 2023 Microsoft Exchange Online Intrusion

March 20, 2024
Cyber Safety Review Board

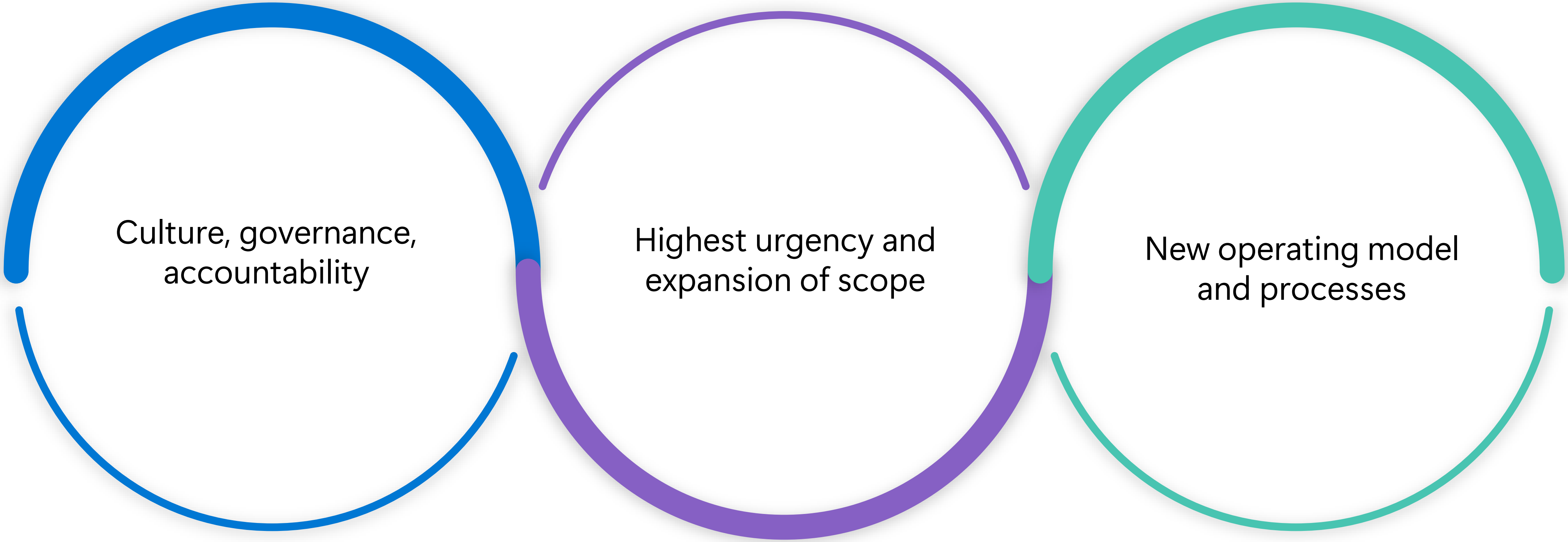
“In the midst of chaos, there is also opportunity” – Sun Tzu

> If you’re faced with the tradeoff between security and another priority, your answer is clear: **Do security**.
>
> —Satya Nadella

# Microsoft Secure Future Initiative

The Microsoft Secure Future Initiative (SFI) is a multiyear initiative to evolve the way we design, build, test, and operate our products and services, to achieve the highest possible standards for security.

# Security above all else



Culture, governance, accountability

Highest urgency and expansion of scope

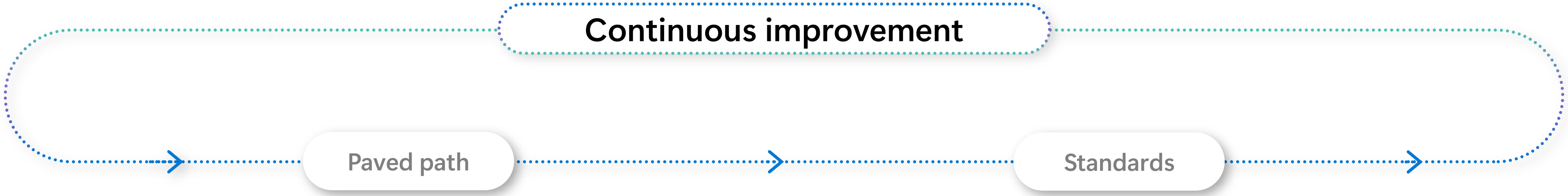
New operating model and processes

# SECURE FUTURE INITIATIVE (SFI)

Secure by design | Secure by default | Secure operations

## Security culture and governance

- Protect identities and secrets
- Protect tenants and isolate production systems
- Protect networks
- Protect engineering systems
- Monitor and detect threats
- Accelerate response and remediation

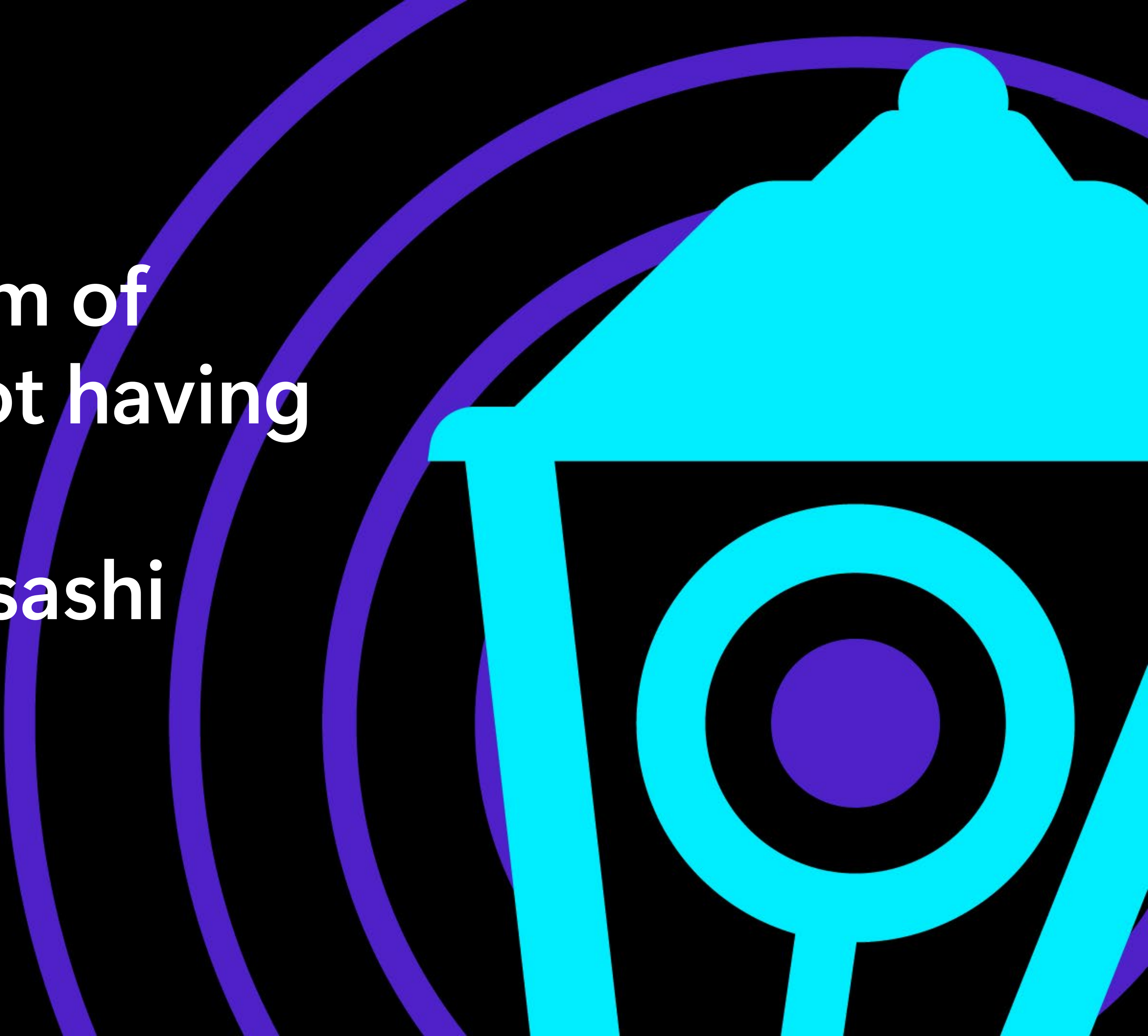


Continuous improvement

Paved path

Standards

“The ultimate aim of martial arts is not having to use them”
– Miyamoto Musashi



# Standards and Paved Paths

Operationalizing an infrastructure project at Microsoft's scale — more than 100,000 engineers, PMs, and designers with over 500,000 work items modified per day and 5 million builds per month — is an enormous task. To scale SFI, drive rapid progress, and to accelerate individual and team productivity, we are leveraging Microsoft Platform Engineering practices and tools.

## What are standards and paved paths

Paved paths are infrastructure and recommended best practices which measurably impact team productivity and the quality of our products. When paved paths move beyond just a recommendation to a requirement, we formalize it as a standard.

## Standards and paved paths in practice

Our strategy for delivering enduring compliance with the standard is to identify how we will Start Right, Stay Right, and Get Right for each standard, which are then driven programmatically through dashboard driven reviews.

**Start Right** equips developers and operators with self-service tools, enabling them to kickstart their projects quickly while adhering to standards defined through templates and policies

**Stay Right** defines automation, policy enforcement, and monitoring to ensure that projects remain compliant with standards

**Get Right** allows us to inventory our estate to understand the current state of compliance and identify areas that require focus to drive to compliance

"Even the finest sword plunged into salt water will eventually rust."
-Sun Tzu

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

# “Shovel Ready”

- Incredibly important to drive initiatives which can actually be achieved
  - Tech Ready
  - Doc Ready
  - Support Ready
- Nothing erodes your initiative faster than “they asked for the impossible”

“The supreme art of war is to subdue the enemy without fighting.”
– Sun Tzu

# Culture and Governance

A security-first culture empowers everyone to take individual responsibility to improve security, which will improve our ability to proactively identify and address security issues as a whole company, not leaving it to our security experts alone.

**Key learning**

Continuous training and discussions geared toward all employees are essential to promoting a security-first mindset across all levels of the organization. Increased governance improvements are critical to maintaining and enhancing our security posture.

## What we are doing

- In May 2024, Satya Nadella emphasized that security is Microsoft's number one priority, a commitment reinforced by integrating cybersecurity performance into the senior leadership team's compensation plans.
- Starting fiscal year 2025, security became a "Core Priority" in performance reviews for all employees, ensuring it remains central to our planning, execution, and governance.
- To support this, continuous training and resources help employees apply a growth mindset to security in their daily work.
- On July 15, 2024, Microsoft launched the Microsoft Security Academy, a personalized learning experience of security-specific, curated trainings for all worldwide employees.

“Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.”
-Sun Tzu

# Principles

These core principles guide our work and help ensure that our products are secure from inception through deployment and ongoing use.

## What are the principles

**Secure by design:** Security comes first when designing any product or service.

**Secure by default:** Security protections are enabled and enforced by default, require no extra effort, and are not optional.

**Secure operations:** Security controls and monitoring will continuously be improved to meet current and future threats.

## Principles in practice

All product teams apply these principles by adopting Microsoft's Security Development Lifecycle (SDL), a practical security approach that is risk-driven and agnostic to development methodology or technology.

### Examples of required processes:

- Perform secure design review and threat modeling.
- Conduct usability testing to encourage secure configurations.
- Perform security testing to assess system security requirements.
- Incorporate threat intelligence feeds into security operations.
- Follow a well-developed and regularly tested incident response plan.

### Examples of resulting product goals:

- Encourage integrated authentication methods and use of Hardware Security Modules (HSM).
- Automate the application of best practices by enforcing automatic updates and conditional access.
- Provide mechanisms that help customers build their security awareness, adopt good security habits, and guard against social engineering and other deceptive attacks.
- Incorporate security logs and the ability to monitor activity into every product.
- Clearly and simply explain security settings and communicate risks of deviating from secure defaults.

“The important thing in strategy is to suppress the enemy's useful actions but allow his useless actions.”
– Miyamoto Musashi

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

# 1. PROTECT IDENTITIES AND SECRETS

Reduce the risk of unauthorized access by implementing and enforcing best-in-class standards across all identity and secrets infrastructure, and user and application authentication and authorization.

### Customer benefits

Eliminate human error, ensuring keys remain inaccessible, thereby safeguarding customer data from potential breaches.

### How pillar maps to CSRB report recommendations:

#6 Secure digital identity systems

#11 Implement modern identity protocols

## What we are doing

- Protect identity infrastructure signing and platform keys with rapid and automatic rotation with hardware storage and protection (i.e., hardware security module (HSM) and confidential compute)
- Strengthen identity standards and drive their adoption through use of standard software development kit (SDKs) across 100% of applications
- Ensure 100% of user accounts are protected with securely managed, phishing resistant multifactor authentication (MFA)
- Ensure 100% of applications are protected with system managed credentials (i.e., Managed Identity/Managed Certificates)
- Ensure 100% of identity tokens are protected with stateful/durable validation
- Adopt more fine-grained partitioning of identity signing keys and platform keys
- Ensure identity and public key infrastructure (PKI) systems are ready for a post-quantum cryptography world

# 1. PROTECT IDENTITIES AND SECRETS

Progress Report - 23rd September 2024

## Standards

**Protect token signing keys using hardware protection to Prevent exfiltration**

**Automatically rotate token signing keys, with no human interaction to prevent mishandling**

**Enforce use of phishing resistant user credentials to prevent account compromise**

**Implement authentication protocols in common implementations and libraries to avoid implementation errors**

**Protect identity tokens with stateful and durable validation to detect forged tokens**

**Remove credentials handling in user account bootstrap and recovery process to prevent credential leaks**

**Use system managed credentials for service-to-service authentication to prevent mishandling and leaks**

**Implement authentication protocols in common implementations and libraries to avoid implementation errors**

## Completed milestones

- ✓ Completed the hardware security module (HSM) based storage implementations for Entra ID and Microsoft Account (MSA) access token signing keys in our public and US Gov clouds
- ✓ Completed the work to deliver automated rotation for Entra ID and Microsoft Account (MSA) application access token signing keys without any human interaction in public and US Gov clouds
- ✓ Completed adoption and enforcement in our production environment for phishing resistant credentials and are in broad adoption across all users in our productivity environment
- ✓ Completed the implementation of Microsoft Authentication Library (MSAL) across core Office Apps across all platforms (iOS, Linux, Windows, MacOS)
- ✓ Completed the work to extend the standardized authentication token logging within our standard identity libraries

## Ongoing effort

- ➢ 95% adoption of video-based user verification (NIST SP 800-63-4) for Microsoft internal productivity environment users
- ➢ Broad adoption of Azure Managed Identity for service-to-service authentication
- ➢ Broad adoption of Identity SDKs across all services at Microsoft. Today, over 73% of tokens issued by Entra ID for Microsoft apps are validated using one standardized implementation

“Build your opponent a golden bridge to retreat across.”
- Sun Tzu

# 2. PROTECT TENANTS AND ISOLATE PRODUCTION SYSTEMS

Protect all Microsoft tenants and production environments using consistent, best-in-class security practices and strict isolation to minimize breadth of impact.

**Customer benefits**

Reduces the attack surface and the possibility for lateral movements.

**How pillar maps to CSRB report recommendations:**

#9 Acquisition security assessments

## What we are doing

- Maintain the security posture & commercial relationships of tenants by removing all unused, aged or legacy systems
- Protect 100% of Microsoft, acquired, and employee-created tenants, commerce accounts and tenant resources to the security best practice baselines
- Manage 100% of Entra ID applications to a high, consistent security bar
- Eliminate 100% of identity lateral movement pivots between tenants, environments, and clouds
- 100% of applications and users have continuous least-privilege access enforcement
- Ensure only secure, managed, healthy devices will be granted access to Microsoft tenants

# 2. PROTECT TENANTS AND ISOLATE PRODUCTION SYSTEMS

Progress Report - 23rd September 2024

## Standards

**Apply governance processes on creation and lifecycle of Entra ID tenants**

**Remove resources managed by Azure Service Management (ASM) API**

**Manage Microsoft Entra ID applications to a high, consistent security baseline to protect resources**

**Maintain inventory and ownership of all Entra ID tenants and applications for effective security investigation and response**

**Isolate credentials and secrets within security boundaries to prevent lateral movement**

**Isolate credentials and secrets within security boundaries to prevent lateral movement**

**Use Just-in-Time (JIT) and Just-Enough-Access (JEA) for privileged administration roles to limit blast radius of compromised accounts**

**Enforce device compliance strictly to protect against and limit impact of device compromise on user identity**

## Completed milestones

- ✓ Implemented a new system to streamline the creation of tenants with secure defaults and strict lifetime management enforced. We have eliminated 5.75 million inactive tenants, drastically reducing the potential attack surface
- ✓ Removed over 440,000 resources which were being managed by the legacy Azure Service Management (ASM) API system
- ✓ Completed a full iteration of lifecycle management for all our production and productivity tenants which eliminated over 730,000 unused apps
- ✓ Completed revising internal system for emergency response
- ✓ Completed a program to restrict access to production environment crash dumps

## Ongoing effort

- ➢ Added controls that isolate application credentials within desired security/tenant boundaries and applied those controls to over 110,000 certificate registrations
- ➢ Enabled automated detection of persistent (as opposed to transient) access to production resources and when possible, automate cleanup or initiate manual investigation
- ➢ Eliminated several classes of tools and business process blockers allowing stricter enforcement of device security compliance standards affecting user access for over 75,000 users. Over 15,000 new production-ready locked-down devices distributed in the last 3 months alone

“You can only fight the way you practice”
- Miyamoto Musashi

# 5. MONITOR AND DETECT THREATS

Comprehensive coverage and automatic detection of threats to Microsoft production infrastructure and services.

### Customer benefits

Real-time threat monitoring, rapid incident response, and complimentary access to security logs ensure a resilient and transparent defense against potential breaches

### How pillar maps to CSRB report recommendations:

#4 Security audit logs for customers

#5 Signing key security

#10 Security audit logs for CSPs

## What we are doing

- Maintain a current inventory across 100% of Microsoft production infrastructure and services
- Retain 100% of security logs for at least 2 years and make 6 months of appropriate logs available to customers
- 100% of security logs are accessible from a central data lake to enable efficient and effective security investigation and threat hunting
- Automatically detect and respond rapidly to anomalous access, behaviors, and configurations across 100% of Microsoft production infrastructure and services

# 5. MONITOR AND DETECT THREATS

## Progress Report - 23rd September 2024

### Standards

**Validate all infrastructure in inventory is emitting sufficient telemetry to support effective security investigation**

**Centrally enforce security log retention period to ensure logs are available to support security investigations over time**

**Provide expanded security logs to customers to support their security investigations and enhance visibility**

**Implement service level security audit logging in standard libraries to ensure all required data is available for security investigation**

**Continue to add effective detections for known tactics, techniques, and procedures (TTPs) to detect threat actor and Red Team simulations and drills**

**Centrally enforce security log retention period to ensure logs are available to support security investigations over time**

### Completed milestones

- ✓ The majority of Microsoft production resources and devices on the backend networks in our inventory are emitting security logs. Over 99% of network devices are now enabled with centralized security log collection and configured to retain for 2 years
- ✓ Established central management and a 2-year retention period for Identity infrastructure security audit logs, encompassing all security audit events throughout the lifecycle of current signing keys
- ✓ Microsoft 365 (M365) audit logs are available to all customers. Enabled more M365 audit logs through Purview. The default free retention period for M365 audit logs has been extended from 90 days to 180 days

### Ongoing effort

- ➢ The majority of Microsoft services are now adopting standard libraries for security audit logs to ensure relevant telemetries are emitted
- ➢ Developing detections based on top TTPs identified through recent security incidents and validating them through continuous attack campaigns and simulations. We have added paging alerts to interaction with signing key systems, added new detections for anomalous app behavior including anomalous authentication patterns, and detections for anomalous authentication to critical resource types
- ➢ In progress of centrally enforcing a minimum of 2-year retention period for all Microsoft production infrastructure and services

# Red Team Engagements are Real Engagements

- We assume breach – if Red Team knows, our adversaries know
- Continuous drilling, hardening, improvement

“Opportunities multiply as they are seized.”
-Sun Tzu

HYBRID
IDENTITY
PROTECTION
conf24
NEW ORLEANS

# SFI progress from November 2023 to May 2024

1M accounts have MFA by default

730K SFI non-compliant apps eliminated

Publish root cause data for Microsoft CVEs using the Common Weakness Enumeration (CWE™) industry standard

270K employees and vendors have enhanced MFA with additional security layers

“Think lightly of yourself and deeply of the world”
- Miyamoto Musashi

# Cybersecurity Governance Council and Microsoft Deputy CISOs

To enhance governance, we have established a new Cybersecurity Governance Council and have appointed Deputy Chief Information Security Officers (Deputy CISOs) aligned to foundational security functions and all engineering divisions.

Deputy CISOs, together with our CISO Igor Tsyganskiy, form the newly established **Cybersecurity Governance Council**. As a group, they take responsibility for the company's overall cyber risk, defense, and compliance.

Each Deputy CISO represents and is accountable for a security domain – an engineering division into which they report, or a foundational security function reporting to the CISO.

### Governance Council Operating Model

The Cybersecurity Governance Council collaborates with SFI engineering leadership to define and prioritize SFI work as well as set future direction.

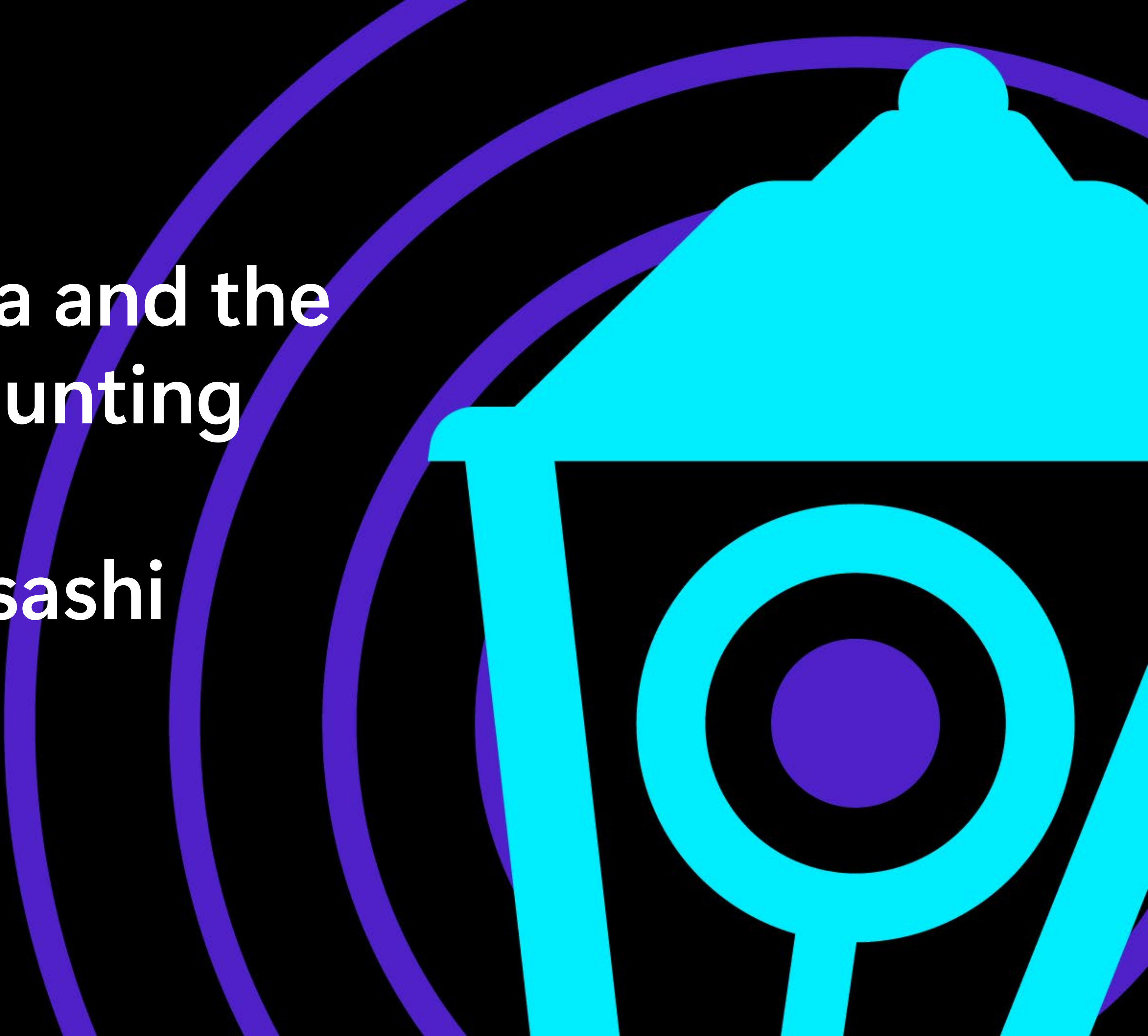
Together, the group reports on cyber risk, compliance, and SFI progress to the CISO, who in turn reports this information to Microsoft's Senior Leadership Team and the Board of Directors.

Tom Burt, Corporate Vice President for Customer Security & Trust, serves as Secretary of the Council for its work specific to regulatory compliance.

## Microsoft Deputy CISOs

- Artificial Intelligence
  Yonatan Zunger, CVP and Deputy CISO
- Azure
  Mark Russinovich, CVP and Deputy CISO
- Consumer
  Kumar Srinivasamurthy, GM and Deputy CISO
- Core Systems and Mergers & Acquisitions
  Geoff Belknap, CVP and Deputy CISO
- Customer Security Management Office
  Ann Johnson, CVP and Deputy CISO
- Experiences and Devices
  Naresh Kannan, Technical Fellow and Deputy CISO
- Gaming
  Shawn Bowen, VP and Deputy CISO
- Government
  Timothy Langan, CVP and Deputy CISO
- Identity
  Igor Sakhnov, CVP and Deputy CISO
- Microsoft 365
  Vanessa Filiberti Bautista, CVP and Deputy CISO
- Microsoft Security
  Terrell Cox, VP and Deputy CISO
- Regulated Industries
  Damon Becknel, VP and Deputy CISO
- Threat Landscape
  John Lambert, CVP and Deputy CISO

“Respect Buddha and the gods without counting on their help”
– Miyamoto Musashi



# SFI progress from May to September 2024

## Culture and Governance

### Significant Investment:

Dedicating the equivalent of 34,000 full-time engineers, SFI is the largest cybersecurity engineering project in history.

### Security as #1 priority:

Security added as a core priority for all employees, measured against all performance reviews. Microsoft's senior leadership team's compensation now tied to security performance.

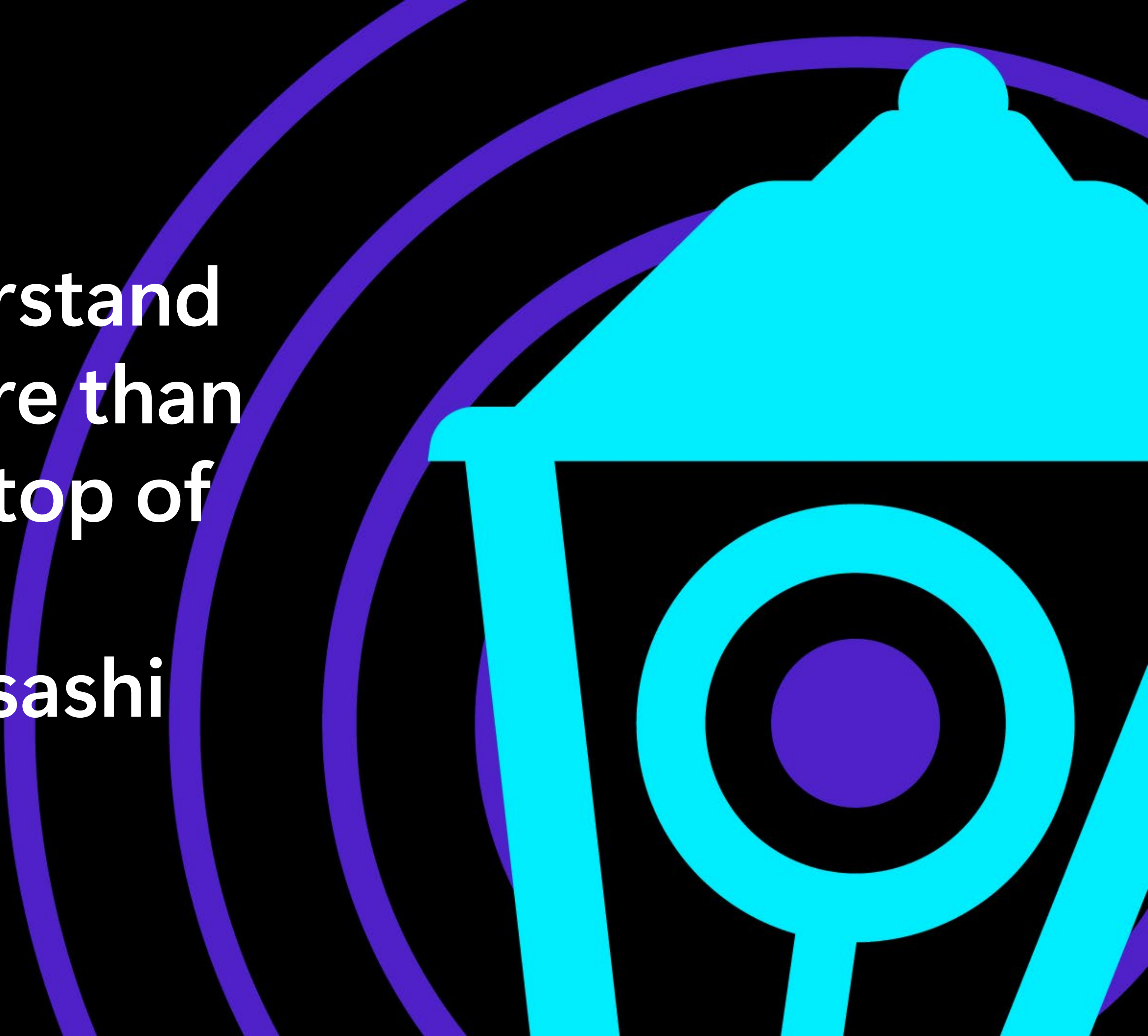
### Security Skilling Academy:

Launched in July, this academy offers curated training for all employees, reinforcing the importance of security in daily operations.

### Governance Enhancements:

- Microsoft's senior leadership team reviews SFI progress weekly and updates are provided to Microsoft's Board of Directors quarterly.
- Introduction of Cybersecurity Governance Council and appointment of Deputy Chief Information Security Officers (Deputy CISOs) aligned with foundational security functions and all engineering divisions to help ensure comprehensive and cohesive security governance.

“You must understand that there is more than one path to the top of the mountain”
– Miyamoto Musashi



HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

# *Questions?*