ISACA
Accra Chapter

11th IT GOVERNANCE SUMMIT

FIESTA ROYALE HOTEL, ACCRA

A BLIND TRUST IN YOUR ZERO TRUST: AN ANALYSIS ON CROWDSTRIKE UPDATE GLITCH

DECODE CHAOS

Desmond Israel ESQ. CISSP, CIPM, CCIT, CC
Founder/Lead Consultant, Information Security Architects Ltd

20TH SEPTEMBER 2024

BIO

ISACA
Accra Chapter

DESMOND ISRAEL ESQ

LLM (Natsec/Cybersec) | LLB | BSc (Mgt. with Computing) | BL | Advanced Diploma (IT)

CISSP | CIPM | CCT | CC | Verified Certificate (Cyberwar, Security and Intelligence)

- ➔ Lawyer and Data Privacy/Information Security Practitioner
- ➔ Founder & Lead Consultant, Information Security Architects Ltd (***Rapid7 & CodeHunter Partner***)
- ➔ Adjunct Lecturer, Ghana Institute of Management and Public Administration (GIMPA) School of Law
- ➔ Consulting Partner, Legal Afrique Unlimited
- ➔ Technology Policy Researcher / Former Fellow (Center for AI and Digital Policy)
- ➔ Research Consultant (Child Online Africa)
- ➔ Memberships: GBA, ISC2, IAPP, IIPGH, ISOC-SIG

A decade and a half, and more in the trenches.

Israel D. Esq.

AGENDA

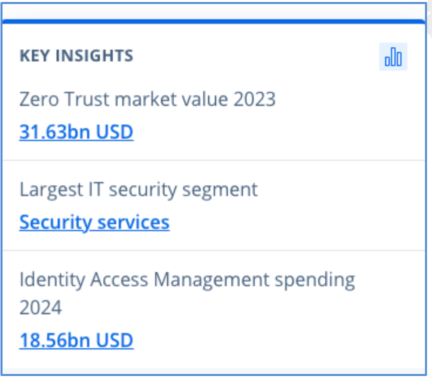
- → Why does it matter?
- → Case Study: The CrowdStrike Update Glitch (a.k.a ***CrowdOut***)
- → Governance Lapses from ***CrowdOut***
- → Understanding Zero Trust Models
- → Implications for Zero Trust Implementations
- → The Illusion of Complete Security
- → Governance and Leadership Responsibilities
- → Lessons to Improve Best Practices
- → Interactive Q&A Session

Why does it matter?

Zero Trust (ZT) Relevant Pointers

1. ZT Market

Expected to be worth nearly 133 billion U.S. dollars by 2032, up from around 32 billion U.S. dollars in 2023.



KEY INSIGHTS

Zero Trust market value 2023
31.63bn USD

Largest IT security segment
Security services

Identity Access Management spending 2024
18.56bn USD

Source: https://www.statista.com/topics/9337/zero-trust/#topicOverview

2. ZT Implementation

In 2024, most companies had already started implementing a formal zero trust strategy or were partnering with multiple security providers to build a roadmap to do so, driven by the need to enable secure remote access for their employees, and modernize their cybersecurity infrastructure.

3. ZT Priority

In 2023, implementing a zero trust model constituted a priority for a large majority of companies.

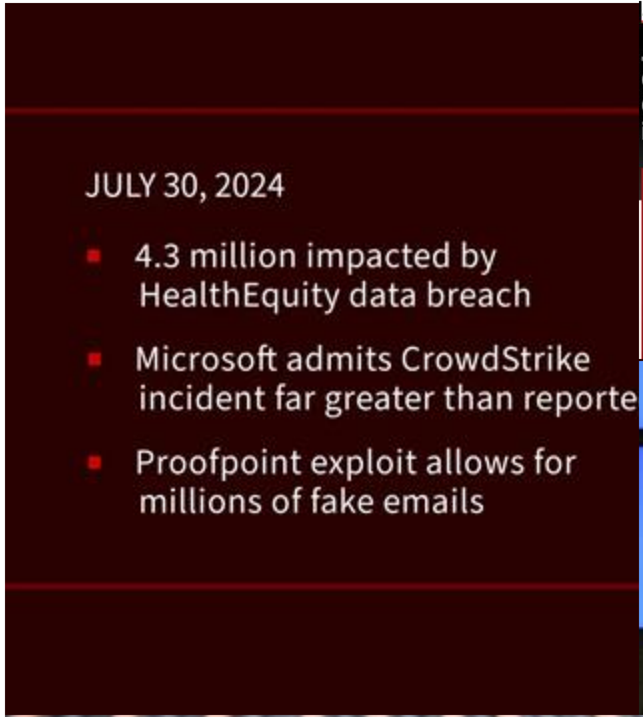
4. SSE Ranking

Security Service Edge (SSE) platforms ranked first in 2024, followed by identity providers.

SSE is the security aspect of secure access service edge (SASE), a cloud-native IT model that combines wide area network edge networking and security services in a way that is better suited, compared to traditional network architectures, to modern business operations.

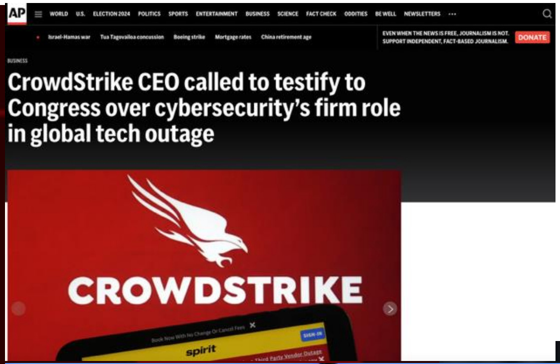
Why does it matter?

ISACA
Accra Chapter



JULY 30, 2024

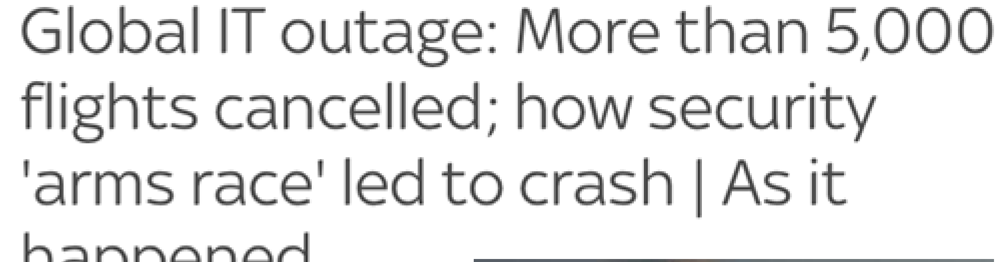
- 4.3 million impacted by HealthEquity data breach
- Microsoft admits CrowdStrike incident far greater than reporte
- Proofpoint exploit allows for millions of fake emails



AP
WORLD U.S. ELECTION 2024 POLITICS SPORTS ENTERTAINMENT BUSINESS SCIENCE FACT CHECK ODDITIES BE WELL NEWSLETTERS ···
Israel-Hamas war Tua Tagovailoa concussion Boeing strike Mortgage rates China retirement age
EVEN WHEN THE NEWS IS FREE, JOURNALISM IS NOT. SUPPORT INDEPENDENT, FACT-BASED JOURNALISM.
DONATE

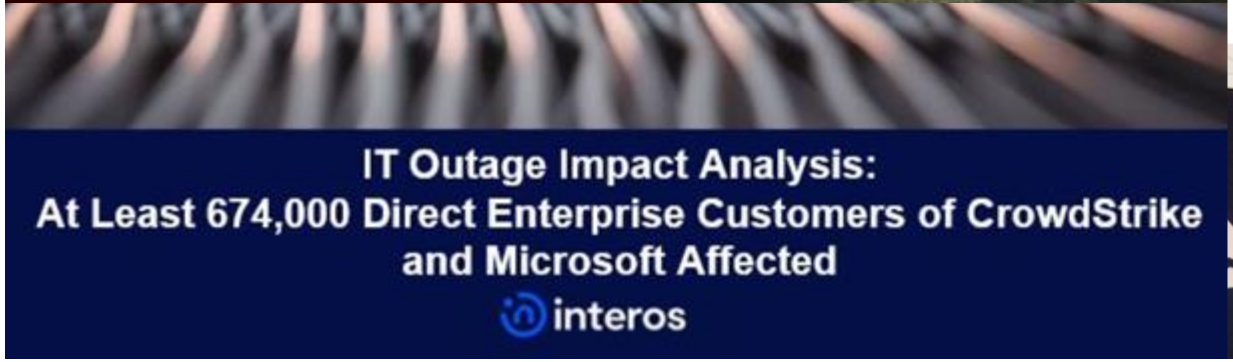
BUSINESS

CrowdStrike CEO called to testify to Congress over cybersecurity's firm role in global tech outage

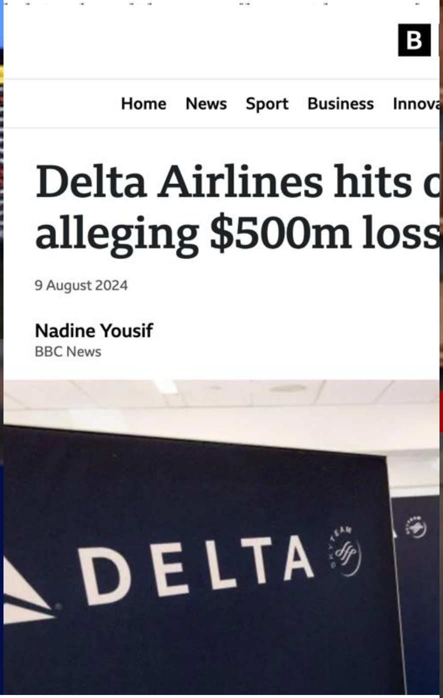


Global IT outage: More than 5,000 flights cancelled; how security 'arms race' led to crash | As it happened

software update has resulted in



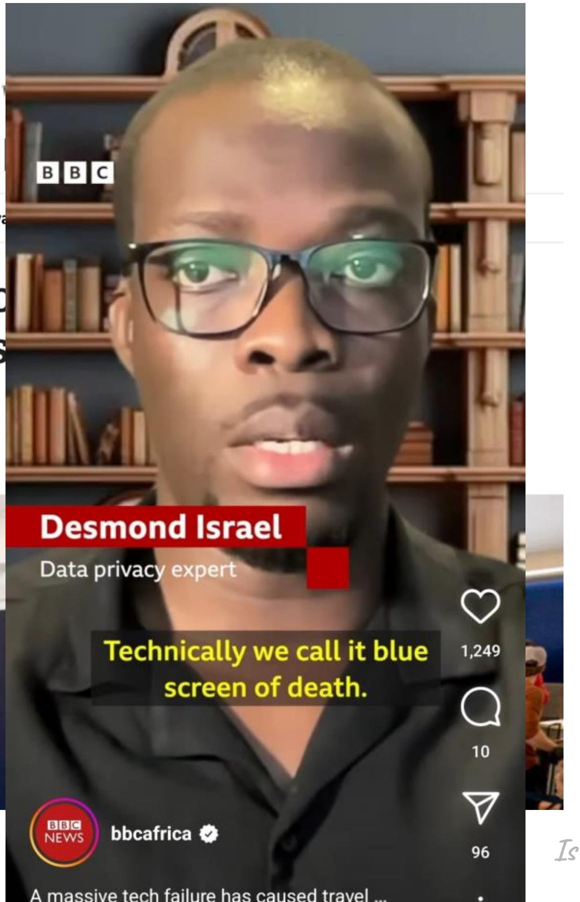
IT Outage Impact Analysis:
At Least 674,000 Direct Enterprise Customers of CrowdStrike and Microsoft Affected



Delta Airlines hits o alleging $500m loss

9 August 2024

Nadine Yousif
BBC News



Desmond Israel
Data privacy expert

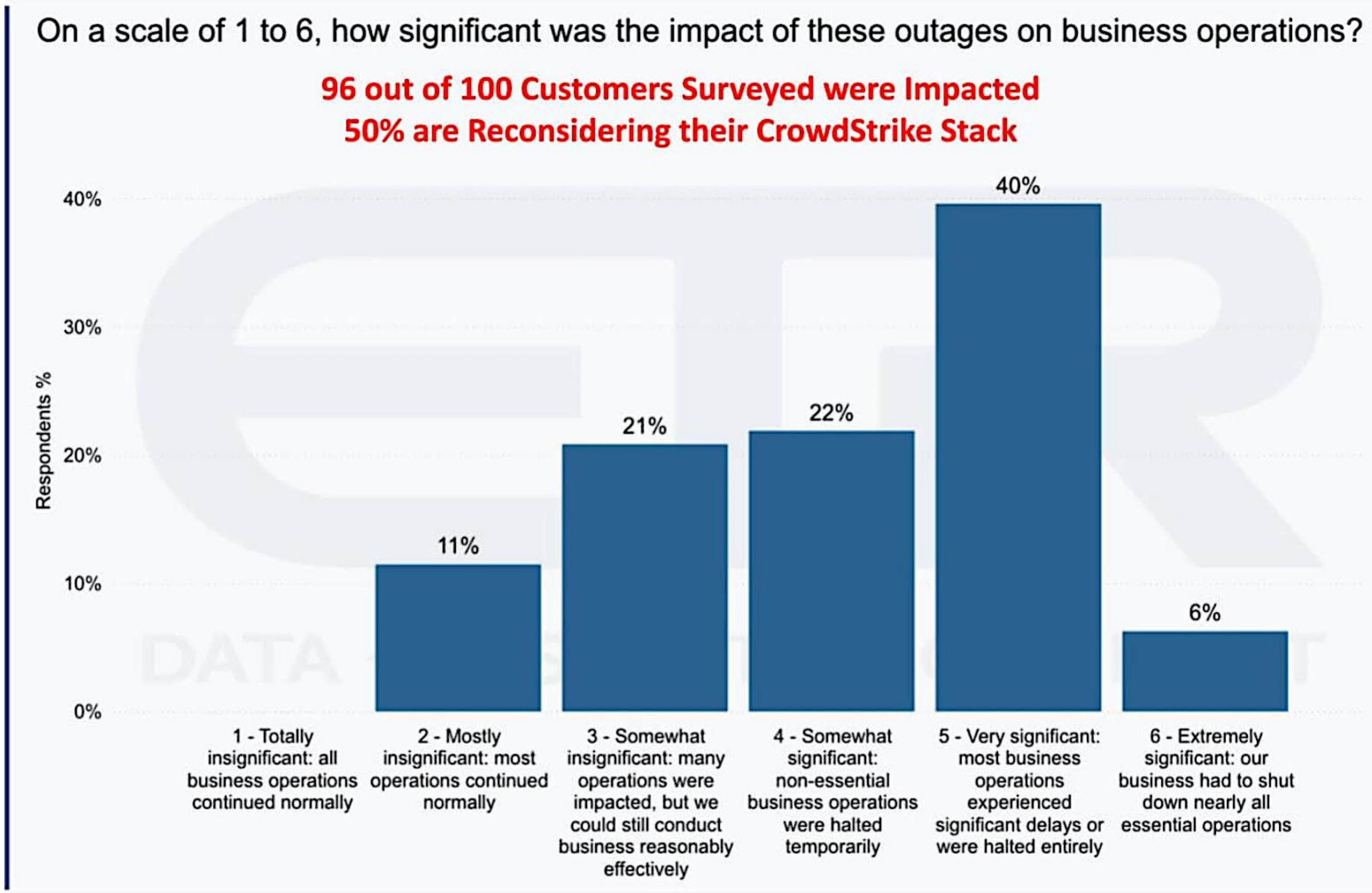
Technically we call it blue screen of death.

A massive tech failure has caused travel ...

Israel D. Esq.

Why does it matter?

ISACA
Accra Chapter



On a scale of 1 to 6, how significant was the impact of these outages on business operations?

96 out of 100 Customers Surveyed were Impacted
50% are Reconsidering their CrowdStrike Stack

Let's take a look at the flash survey results from ETR.

ETR asked **100 CrowdStrike customers** the question, "Were you impacted by this incident?"

Ninety-six percent (96%) out of that a hundred said they were impacted.

Israel D. Esq.

Case Study: ***CrowdOut***

Faulty update they say!!

System Crash

Faulty content update of the CrowdStrike Falcon Sensor causes Blue Screen of Death (BSoD)

July 19

Patch Released

CrowdStrike officially issues a patch and workaround for remediation.

July 19

Production Fix

CrowdStrike adds the fix to its regular product update release.

July 27

Case Study: *CrowdOut*

ISACA
Accra Chapter

CROWDSTRIKE

Falcon Sensor Content Update Released

1

Falcon Sensor Agent is updated on Microsoft Operating Systems

2

Content Update within the Falcon sensor attempts to use its defined Channel File 291 for content validation

CROWDSTRIKE

3

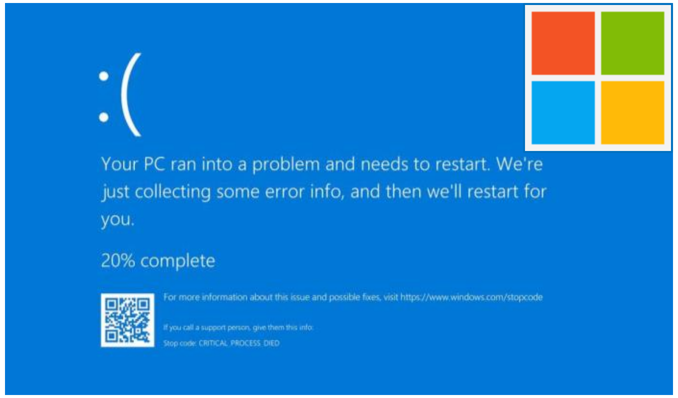
The Template type expected a 20-parameter input, but the Content Interpreter with Channel File 291's Template Instances supplied 21 input values to match against.

CROWDSTRIKE

4

The parameter mismatch causes Microsoft Windows to go into failsafe mode which was seen as a BSoD

5



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

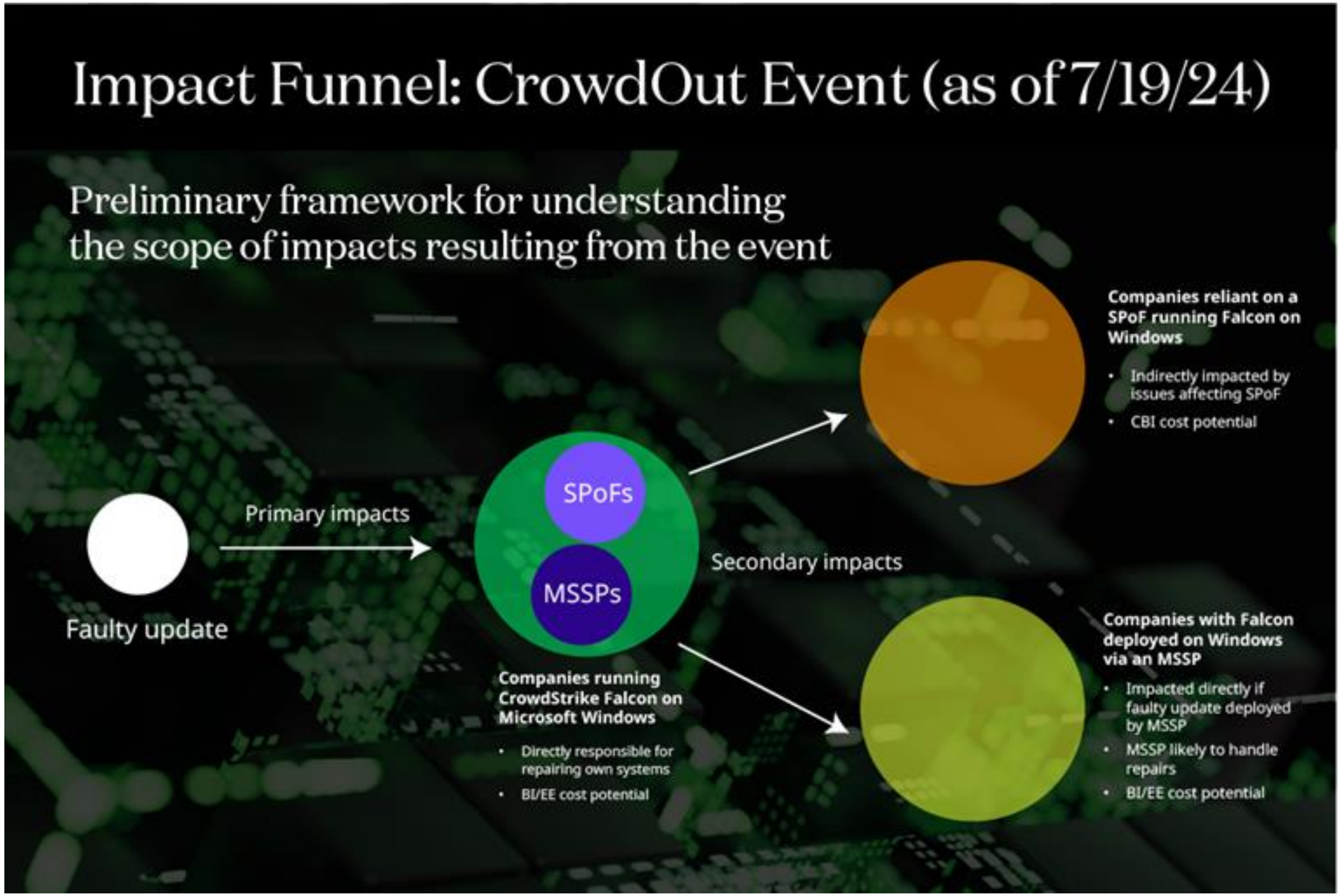
If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

These AI-backed models are kept up-to-date and strengthened with learnings from the latest threat telemetry from the sensor and human intelligence from **Falcon Adversary OverWatch**, **Falcon Complete** and **CrowdStrike threat detection engineers**.

Israel D. Esq.

Case Study: *CrowdOut*



Impact Funnel: CrowdOut Event (as of 7/19/24)

Preliminary framework for understanding the scope of impacts resulting from the event

Companies running CrowdStrike Falcon on Microsoft Windows

- Directly responsible for repairing own systems
- BI/EE cost potential

Companies reliant on a SPoF running Falcon on Windows

- Indirectly impacted by issues affecting SPoF
- CBI cost potential

Companies with Falcon deployed on Windows via an MSSP

- Impacted directly if faulty update deployed by MSSP
- MSSP likely to handle repairs
- BI/EE cost potential

Source: *businesswire.com*

The faulty CrowdStrike Falcon Sensor update and subsequent outage – *the CrowdOut Event* – underscore the potential for **Single Point of Failure (SPoF) technology** outages to impact the global digital economy.

Exposing companies that rely on these SPoFs to a possible **Contingent Business Interruption (CBI)** outages.

This is mainly **a system failure or Business Interruption (BI)** event

Israel D. Esq.

Case Study: *CrowdOut*

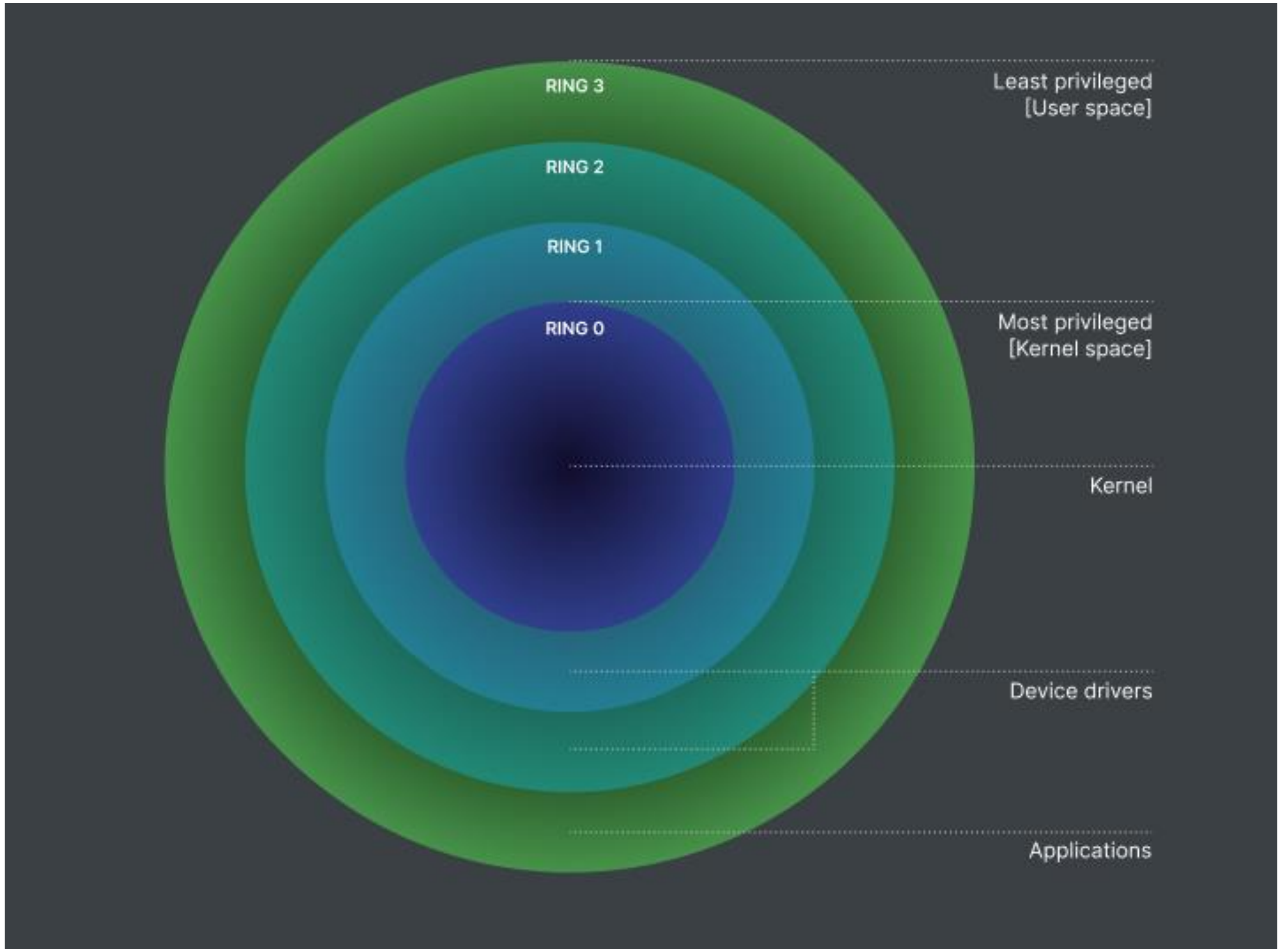
ISACA
Accra Chapter

Let’s go back into time…

A 2009 Agreement between the European Commission and Microsoft required that they **give security software the same level of access to Windows as Microsoft itself**.

This meant that Microsoft **could not make security changes that would have blocked the update** from cybersecurity firm CrowdStrike.

The impact was a system crash that caused an estimated **8.5 million computers to fail.**



Israel D. Esq.

Governance Lapses from *CrowdOut*

Software Development Lifecycle (SDLC) Governance

Issue: The lack of a specific test to catch the input mismatch indicates weaknesses in the SDLC processes.

Explanation: Effective SDLC governance requires rigorous testing protocols, including unit, integration, and regression testing. The absence of tests that could have detected the out-of-bounds read issue suggests gaps in quality assurance and testing procedures.

Change Management Failures

Issue: The deployment of Channel File 291 containing problematic content without adequate validation.

Explanation: Proper change management involves assessing the impact of updates, thorough testing, and approval before implementation. The failure to detect issues in Channel File 291 indicates insufficient change control mechanisms.

Risk Management Oversight

Issue: Inadequate identification and mitigation of risks associated with updates to critical security software.

Explanation: Governance frameworks require ongoing risk assessments, especially when deploying changes that could affect system stability. The incident reflects a lapse in proactive risk management practices.

Third-Party Collaboration Governance

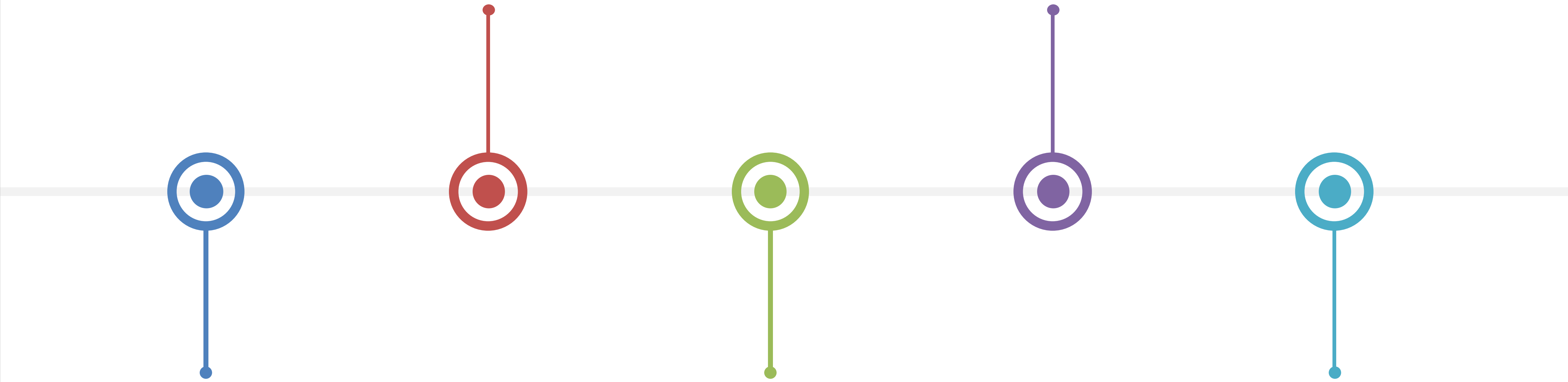
Issue: The need for better coordination between CrowdStrike and Microsoft to ensure compatibility and security.

Explanation: Effective governance includes managing third-party relationships to ensure integrated systems function securely. The incident underscores the importance of collaborative governance structures with key partners.

Israel D. Esq.

Understanding Zero Trust Models

How we arrived here…



The corporate enterprise **perimeter is eroded by remote and hybrid work** environments

Let’s bring in enterprise **security designed as though there is no traditional network** edge.

Make enterprise **resource accessible anywhere,** and **anytime** from any device

”Never trust, always verify” meaning no default trust for user and device.

Assume breach

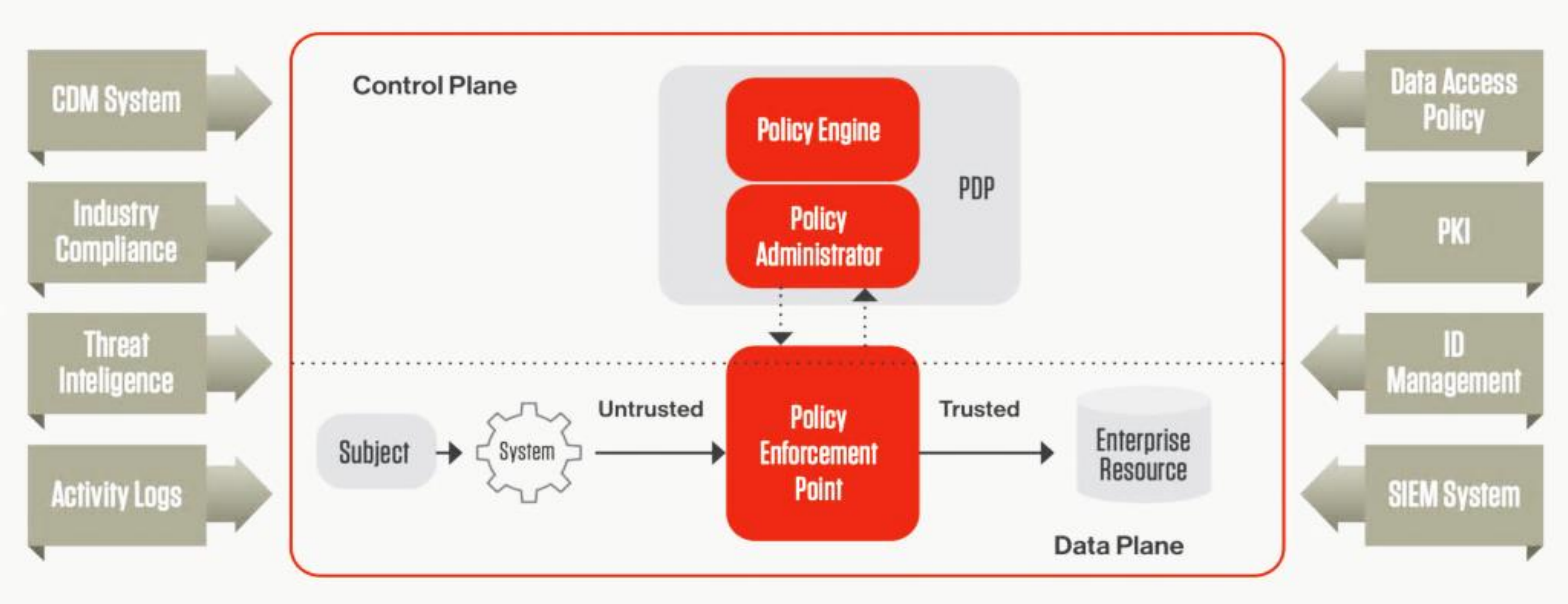
Zero Trust arrived as a cybersecurity strategy **based on eliminating any trust within an environment** regardless of location.

Israel D. Esq.

Understanding Zero Trust Models

ISACA
Accra Chapter

Zero Trust Architecture (ZTA) also know as the Zero Trust Framework (ZTF)



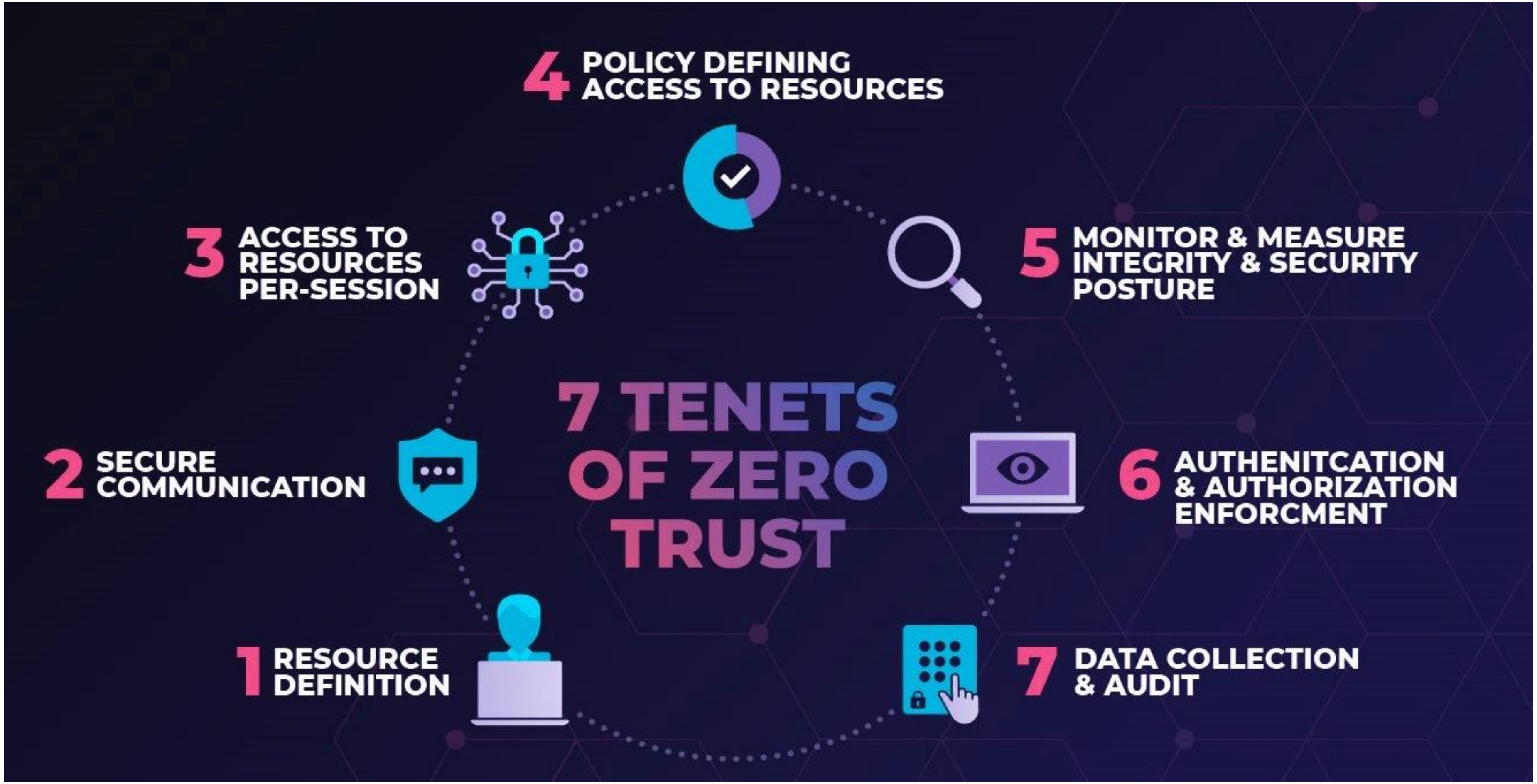
NIST Special Publication 800-207:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Israel D. Esq.

Understanding Zero Trust Models

ISACA Accra Chapter

The Seven (7) Tenets of Zero Trust (ZT)



4 POLICY DEFINING ACCESS TO RESOURCES
3 ACCESS TO RESOURCES PER-SESSION
5 MONITOR & MEASURE INTEGRITY & SECURITY POSTURE
7 TENETS OF ZERO TRUST
2 SECURE COMMUNICATION
6 AUTHENITCATION & AUTHORIZATION ENFORCMENT
1 RESOURCE DEFINITION
7 DATA COLLECTION & AUDIT

NIST Special Publication 800-207: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Implications for Zero Trust Implementations

Critical Assessment of Zero Trust Models (ZTM)

Strengths	Weakness
Continuous Authentication: Zero Trust demands constant verification, which reduces the risk of malicious actors gaining unauthorized access through compromised credentials.	**Complexity in Implementation:** The transition to a Zero Trust model can be technically and operationally complex, requiring comprehensive network restructuring, policies, and a high level of IT expertise.
Least Privilege Access: Users and devices are granted the minimum necessary access to resources, limiting the scope of potential damage in the event of a breach.	**Resource-Intensive:** Due to the continuous verification mechanisms and the monitoring tools required, ZTM can be resource-heavy, both in terms of finances and computing power. This might be particularly difficult for small or resource-constrained organizations.
Micro-segmentation: By breaking down network zones into smaller parts, ZTM prevents lateral movement across a network, meaning even if one part of the system is compromised, it doesn't automatically expose the whole network.	**User Friction:** Requiring continuous authentication can lead to friction for users who may find frequent logins, multi-factor authentication (MFA), or restricted access cumbersome and inefficient, potentially slowing productivity.
Increased Visibility: Zero Trust models often incorporate advanced monitoring and analytics, which provide greater visibility into user behaviors, network activity, and potential threats.	**Initial Trust Assumptions:** While Zero Trust advocates for a "never trust, always verify" stance, there are still inherent trust assumptions, especially in the initial onboarding process or the configuration of endpoints, which can become attack vectors.
Adaptability: ZTM is scalable and can be tailored to suit various industries, whether they be traditional IT environments, cloud infrastructures, or hybrid models.	

The Illusion of Complete Security

ISACA Accra Chapter

Blind Spots in Zero Trust Models

Insider Threats: Insiders with legitimate access may still pose significant risks. (Privilege abuse or Account compromise)

Legacy Systems: Mostly cannot integrate seamlessly into a Zero Trust framework they become blind spots since they often don't support modern authentication or segmentation methods.

Cloud Integration: Cloud workloads and data often reside in hybrid integration (multi-cloud environments) where a fully centralized Zero Trust model is difficult to implement.

Blind Trust in Zero Trust Models

CROWDSTRIKE

Trusted Third Parties: Reliance on cloud service providers (CSPs), identity providers (IdPs), or third-party security vendors for Zero Trust architecture components. However, blind trust in these third parties can become problematic if they suffer from risk mistakes, operational flaws, process gaps, vulnerabilities or get compromised themselves.

Predefined Rules & Policies: While access is based on strict policies, these policies are still created and maintained by humans. Misconfigurations or overly permissive rules can inadvertently lead to blind trust in certain users, devices, or network segments, *undermining the Zero Trust principle.*

Device Trust: Endpoints are often trusted after initial verification. However, if devices become compromised after authentication (e.g., through malware), they may retain access privileges longer than they should, *creating a blind spot.*

Israel D. Esq.

Governance and Leadership Responsibilities

ISACA
Accra Chapter

Policy Development and Enforcement

Concern: Crafting comprehensive security policies that align with Zero Trust principles can be complex. Ensuring these policies are consistently enforced across all departments and systems is critical to prevent security gaps.

Change Management and Organizational Culture

Concern: Transitioning to a Zero Trust Model requires significant cultural and behavioral changes within an organization, necessitating effective change management strategies.

Insider Threat Management

Concern: Employees with legitimate access can misuse their privileges, either maliciously or inadvertently, posing significant security risks that are challenging to monitor without infringing on privacy.

User Experience and Productivity Impact

Concern: Continuous authentication and strict access controls may hinder user productivity, leading to frustration and potential non-compliance with security protocols.

Legacy Systems and Technology Integration

Concern: Integrating outdated legacy systems that may not support modern security protocols can create vulnerabilities and hinder the implementation of a cohesive Zero Trust strategy.

Third-Party and Supply Chain Risks:
Concern: Dependence on external vendors and service providers introduces risks that need to be managed through robust governance frameworks and due diligence processes.

CROWDSTRIKE

Israel D. Esq.

Lessons to Improve Best Practice

- **Review and Strengthen SDLC Processes:** Implement comprehensive testing strategies, including automated and manual tests, to catch potential issues early.
- **Enhance Change Management Controls:** Establish rigorous approval processes for updates and changes, with thorough impact assessments.
- **Conduct Regular Dependency Risk Assessments:** Continuously evaluate risks associated with software dependencies and third-party integrations.
- **Contracts and SLAs Review and Clarification:** Ensure that responsibilities and expectations are explicitly defined to prevent disputes.
- **Review and Update Incident Response Plans:** Create detailed procedures for responding to incidents, including clear communication channels with clients and partners.
- **Invest in Quality Assurance:** Engage independent auditors and reviewers to validate code/services quality and security.
- **Promote Collaborative Governance:** Foster partnerships with key stakeholders, including technology providers, to align on security practices and standards.

THANK YOU

desmond@isa.com.gh

desmond.israel@gmail.com

Linkedin.com/in/desmondisrael

@desmond_israel