

ISSA CENTRAL MARYLAND CHAPTER • TECHNICAL KEYNOTE

Behaviors as Artifacts: Redefining Software Identity in the Age of AI

Operationalizing Intent and Behavioral Intelligence

Jared Sladich

Technical Concepts Session

Jared Sladich: Technical Solutions Guy



linkedin.com/in/jared-sladich

CORE IDENTITY

20+ Years Operations

Driving strategic and tactical success across DoD, Intelligence Community, and Enterprise Private Sector.

Dual Domain Expert

Mastering both **Human Intelligence (HUMINT)** tradecraft and advanced **Cybersecurity** operations.

Technical Solutions

Bridging high-level Sales Engineering, Product Strategy, and Technical Execution.

HUMAN INTELLIGENCE

- Source Operations & Interrogation
- Tactical & Strategic Missions
- Sensitive Site Exploitation (SSE)
- Multi-lingual Operations

CYBERSECURITY

- Digital Forensics (DCITA)
- Cyber Counterintelligence
- Zero Trust & Cyber HUNT
- Threat Intelligence Product Dev

Reframing the Core Cybersecurity Question

Moving beyond static identifiers toward understanding software by how it acts, regardless of name, hash, or origin.

Legacy Perspective: Identity & Reputation

PRIMARY QUESTION

"Have I seen this file before?"

Focuses on static wrappers, file hashes, signatures, and pre-assigned reputation metrics. Vulnerable to simple renaming, obfuscation, or zero-day variants.

Modern Paradigm: Behavioral Intent

EVOLVED QUESTIONS

"Have I seen this behavior before?"
"Does this behavior belong in my environment?"

Evaluates real-time execution logic, operational conduct, and contextual authorization regardless of file metadata or origin.

STRATEGIC IMPLICATION

Software identity is no longer defined by static packaging, but by runtime intent and operational effect within the ecosystem.

The Metadata Fallacy: Packaging vs. Capability



Physical Metadata Model

Inspects static wrappers:
hashes, file names, PE headers, and
digital certificates.

Core Question: "What is this file?"

Human Analogy: ID number, height,
hair and eye color.



Behavioral Artifact Model

Extracts underlying execution logic:
token manipulation, injection, and egress
channels.

Core Question: "What does it do in
this environment?"

Human Analogy: Conduct, intent, and
cognitive decision.

Evolve the Traditional Lifecycle: Blending Intent Throughout

PHASE 01

Identification

Capability whitelisting establishes authorized software behaviors before deployment.

PHASE 02

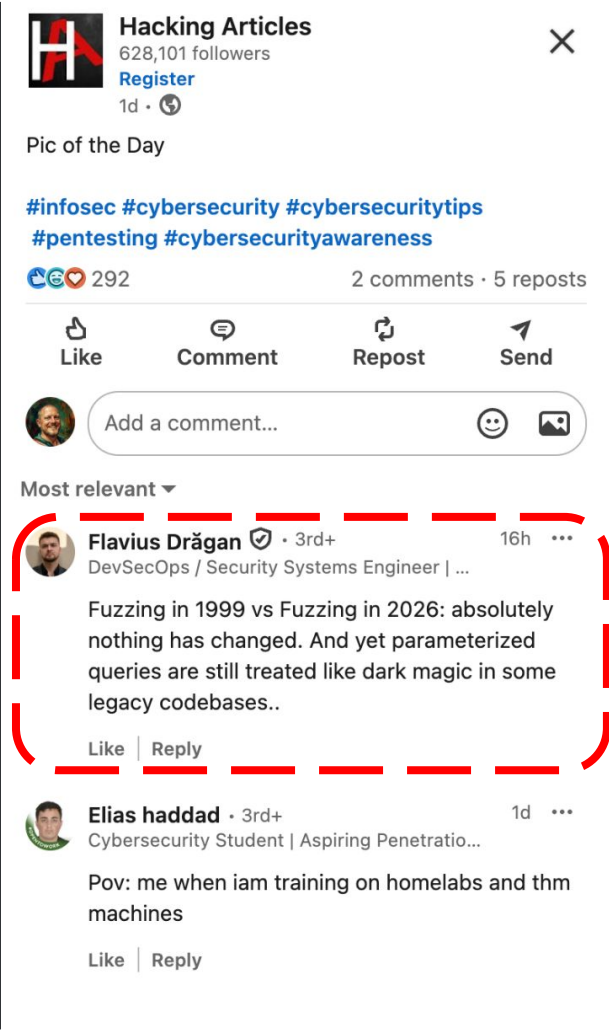
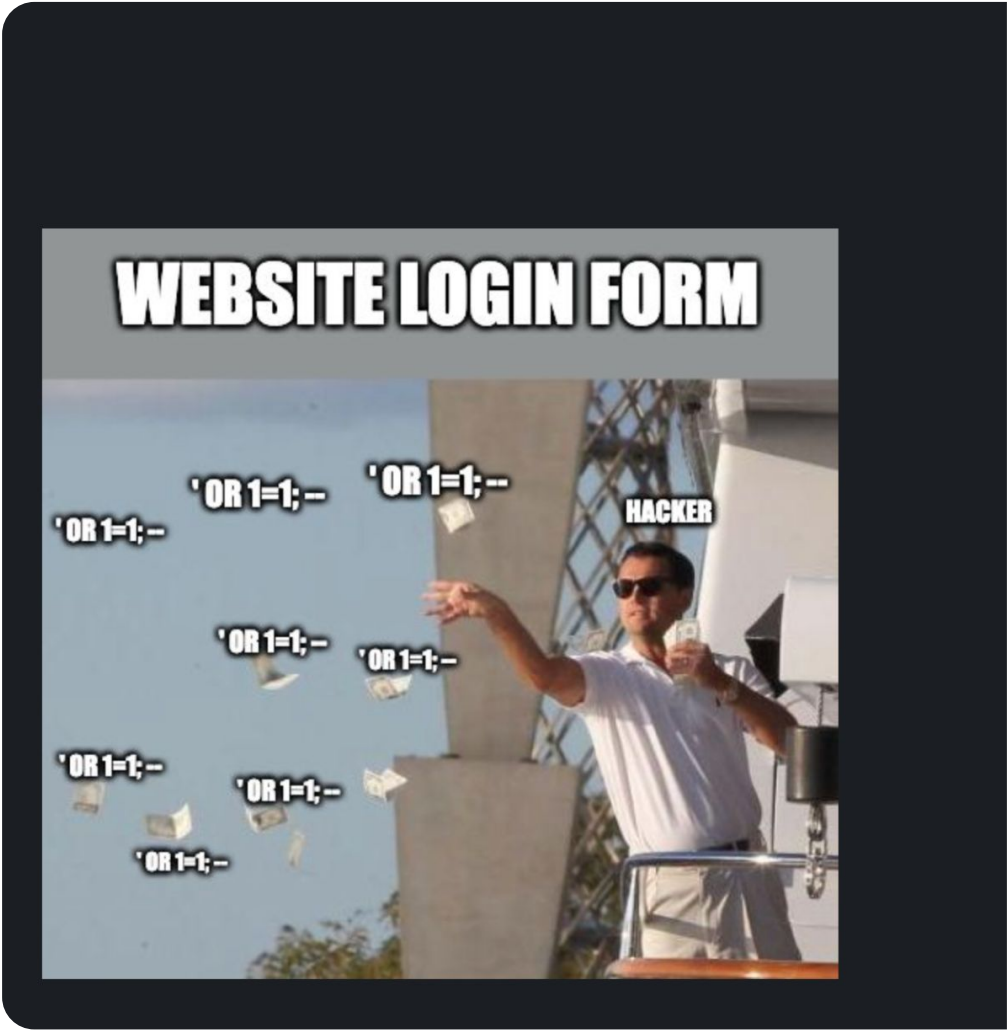
Detection

Maps anomalous events against adversary tradecraft to extract underlying intent.

PHASE 03

Remediation

Neutralizes rogue threads, invalidates hijacked tokens, and revokes persistence hooks.



Deterministic Sifting: The Enduring Value of Signatures

Behavioral analysis does not discard static signatures. Traditional controls eliminate commodity noise at machine speed.

$O(1)$

Constant-Time Lookup

Instant hash queries against billions of known records.

90%+

Commodity Filtration

Sieves mass opportunistic threats without dynamic sandbox delays.

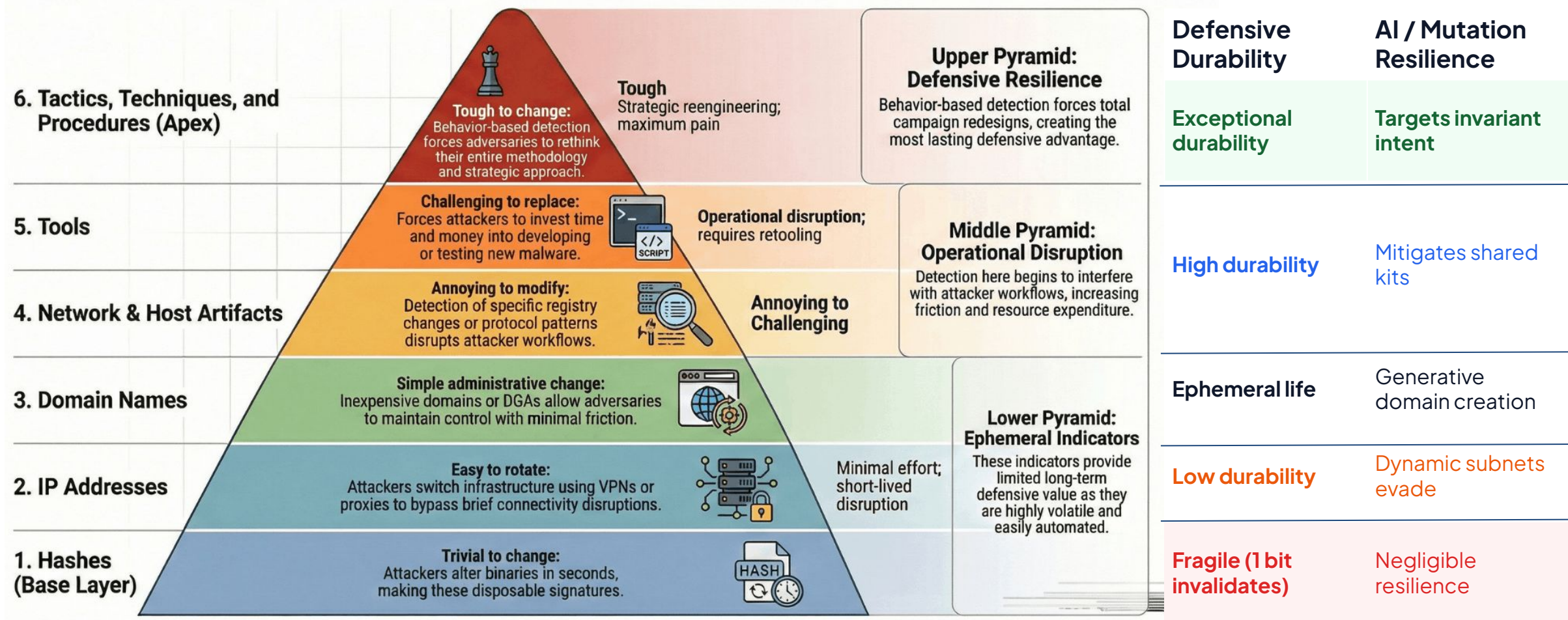
0 ms

Zero Sandbox Detonation

Conserves high-overhead behavioral engines for unknown payloads.

The Pyramid of Pain: Where Defense Gains Leverage

The Pyramid of Pain: Understanding Attacker Cost in Cybersecurity Detection



Pre-Execution Visibility: Deriving Intent Prior to Runtime

01

Static Ingestion

Raw binaries, scripts, or container bytecodes.

02

CFG Reconstruction

Automated disassembly traces control flows.

03

Capability Extraction

Uncovers signature masking, injection, and evasion.

04

Deterministic Verdict

Allow, Block, or Quarantine prior to execution.

963f9ee4_mod_hermeticwiper.exe

MALICIOUS

SHA256

963f9ee48ab351f46703da6f3a4aad5f4d98d91dcac20b556353111b9910fc90

Identified Behaviors

Network Details

Executive Summary

Critical

3

27

Medium

16

27

Low

8

27

Detailed analysis mapped the following behaviors, uncovering possible interactions, modifications, and execution pathways.

Search Behavior Name

Filters

Known Advanced Persistent Threat Artifact

Critical

Defense Evasion: Disable Or Evade Security Tools

Critical

Rootkit Installation: Bootloader

Critical

System Information Discovery

Medium

Remote Commands: System Shutdown

Medium

Interact With Driver Via IOCTL

Medium

Persistence: Modify Existing Service

Medium

Command And Scripting Interpreter: Parse Command Line Arguments

Medium

File And Directory Discovery

Medium

Known Advanced Persistent Threat Artifact

Critical

Description

Analysis matched an artifact signature utilized by an Advanced Persistent Threat actor.

Evidence

YARA

SIGNATURE_BASE_APT_UA_HERMETIC_WIPER_FEB22_1

RuleVersion: -

Credit: CodeHunter

Machine-Speed Polymorphism: The Signature Collapse

AST & Control-Flow Mutation

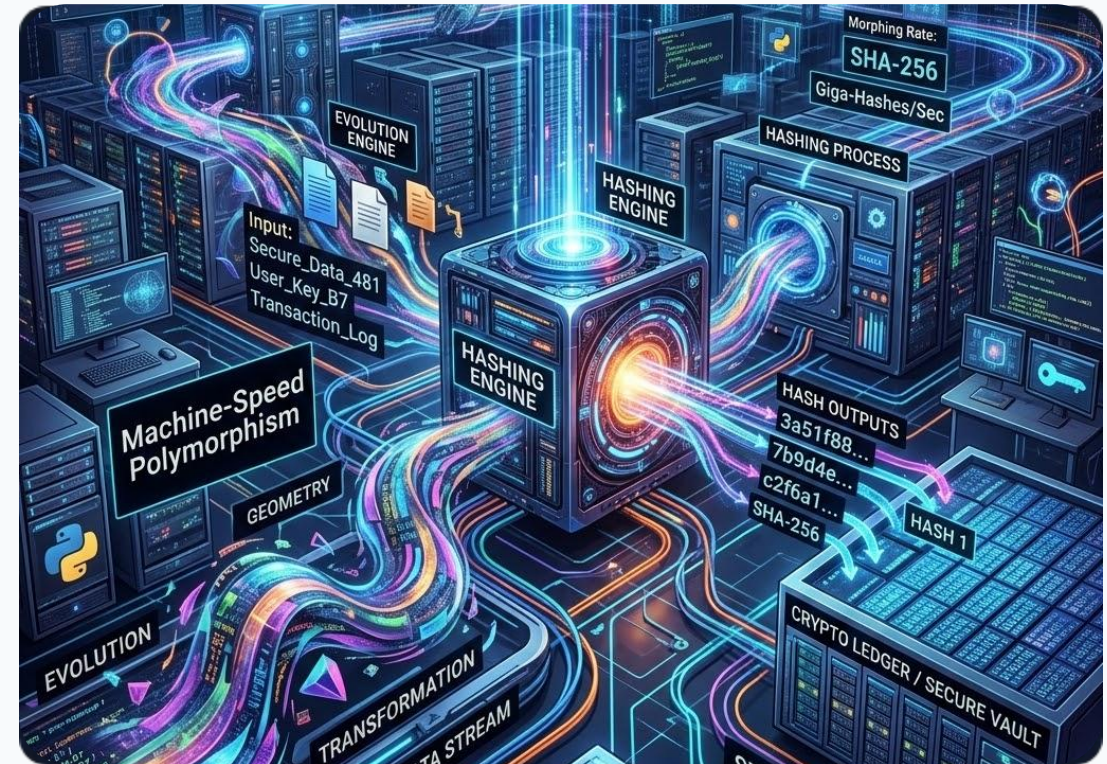
Compilers reorder execution branches while preserving core exploit payloads.

Runtime Dynamic API Resolving

Payloads walk the Process Environment Block (PEB) and hash API strings to bypass static import tables.

One-Off Cryptographic Hashes

Every emitted binary produces a novel SHA-256 digest, nullifying static blocklists.



Living off the Land: The Ghost in the System



Signed Binaries

Authentic Microsoft certificates verify identity.



Zero Malware on Disk

Executes purely in-memory via LOLBins.



Contextual Execution

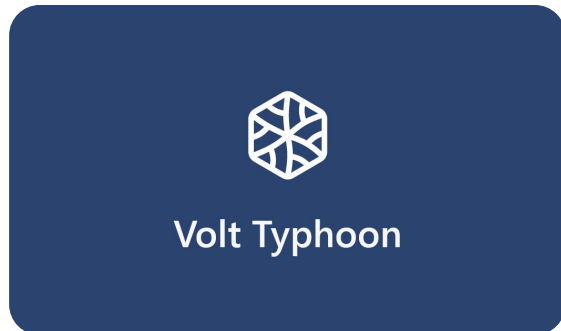
Parent-child lineage exposes threat intent.

When Static Verification Fails: Three Critical Incidents

CRITICAL INFRASTRUCTURE

Volt Typhoon

Deployed zero custom binaries. Leveraged native tools like ntdsutil.exe to dump Active Directory credentials into temporary paths.



Static Antivirus verdict: Benign Microsoft tool.

SUPPLY CHAIN (CVE-2024-3094)

XZ Utils Backdoor

M4 build scripts hooked OpenSSH authentication routines. Official source archives carried verified signatures and passed security checks.



Detected via: 500ms CPU latency anomaly.

TRUST SUBVERSION

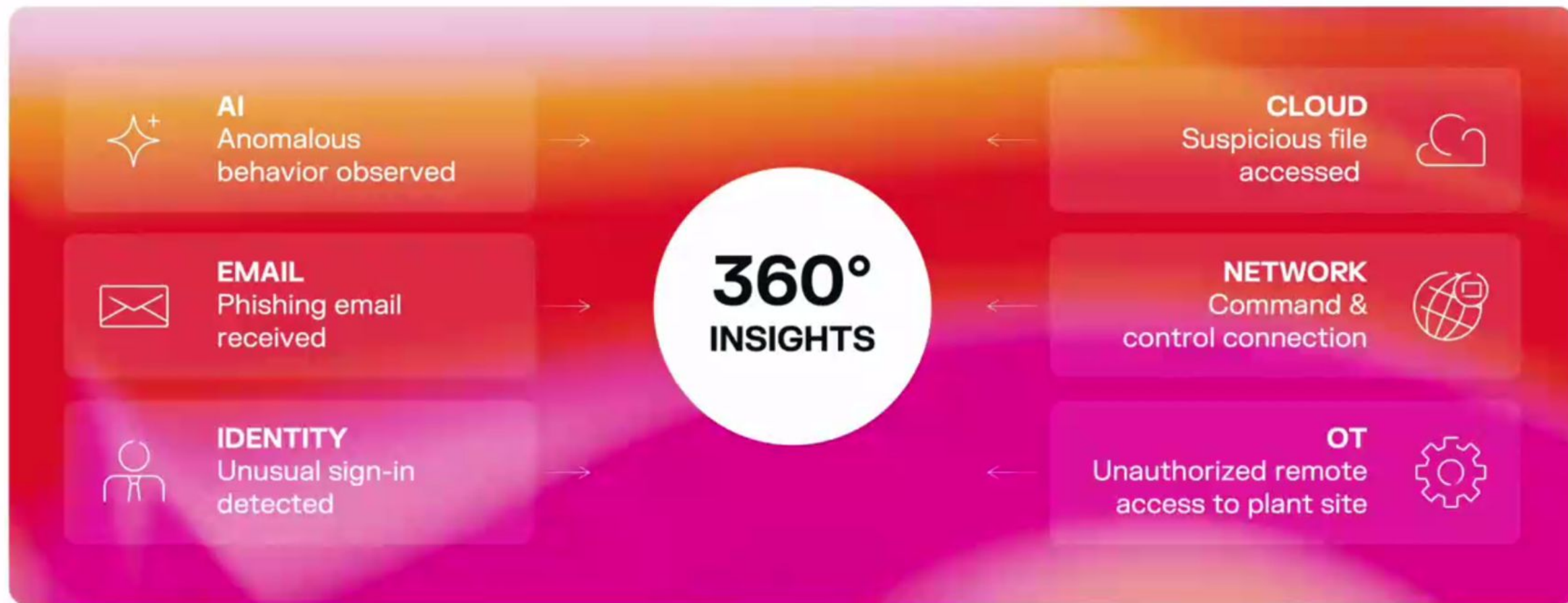
SolarWinds SUNBURST

Backdoor compiled inside legitimate DLL, signed with authentic certificate. Remained dormant for weeks to outlast automated sandbox timers.



Signature confirmed origin; behavior exposed intent.

Dynamic Pattern-of-Life: Environmental Baselines



CORRELATED VISIBILITY TURNS ACTIVITY ACROSS AI, PEOPLE, & INFRASTRUCTURE INTO ONE SECURITY STORY.

AI TECHNIQUES

Anomaly Detection

Probabilistic Reasoning

Graph Analysis

Large Language Models

and dozens of other proprietary
and advanced AI techniques



ADAPTIVE AI

Continuously
learns from your
unique business

BUSINESS CONTEXT

Behaviors

How people, systems, and AI typically act

Relationships

How identities, applications, and assets connect

Operational Patterns

How activity unfolds over time

Adaptive AI Continuously Learns How Your Business Operates

IT'S DANGEROUS TO GO ALONE! TAKE THIS.

Strategic Takeaways: The Behavioral Imperative

- Maintain traditional metadata and cryptographic lookups as essential filters for commodity hygiene.
- Recognize that against AI-synthesized polymorphism, living-off-the-land techniques, and supply chain attacks, static identity provides only baseline security.
- Build and maintain behavioral catalogs that continuously evaluate, classify, and audit what software is programmed to execute.
- Keep your Engineers happy.

ISSA CENTRAL MARYLAND CHAPTER • FLOOR DISCUSSION

Technical Exchange & Audience Inquiries

Understanding and predicting software behaviors is paramount in defending against threats generated at AI speed.

Always remember that there is human intent.

Jared Sladich
Technical Solutions Guy

LinkedIn & Connect
linkedin.com/in/jaredsladich