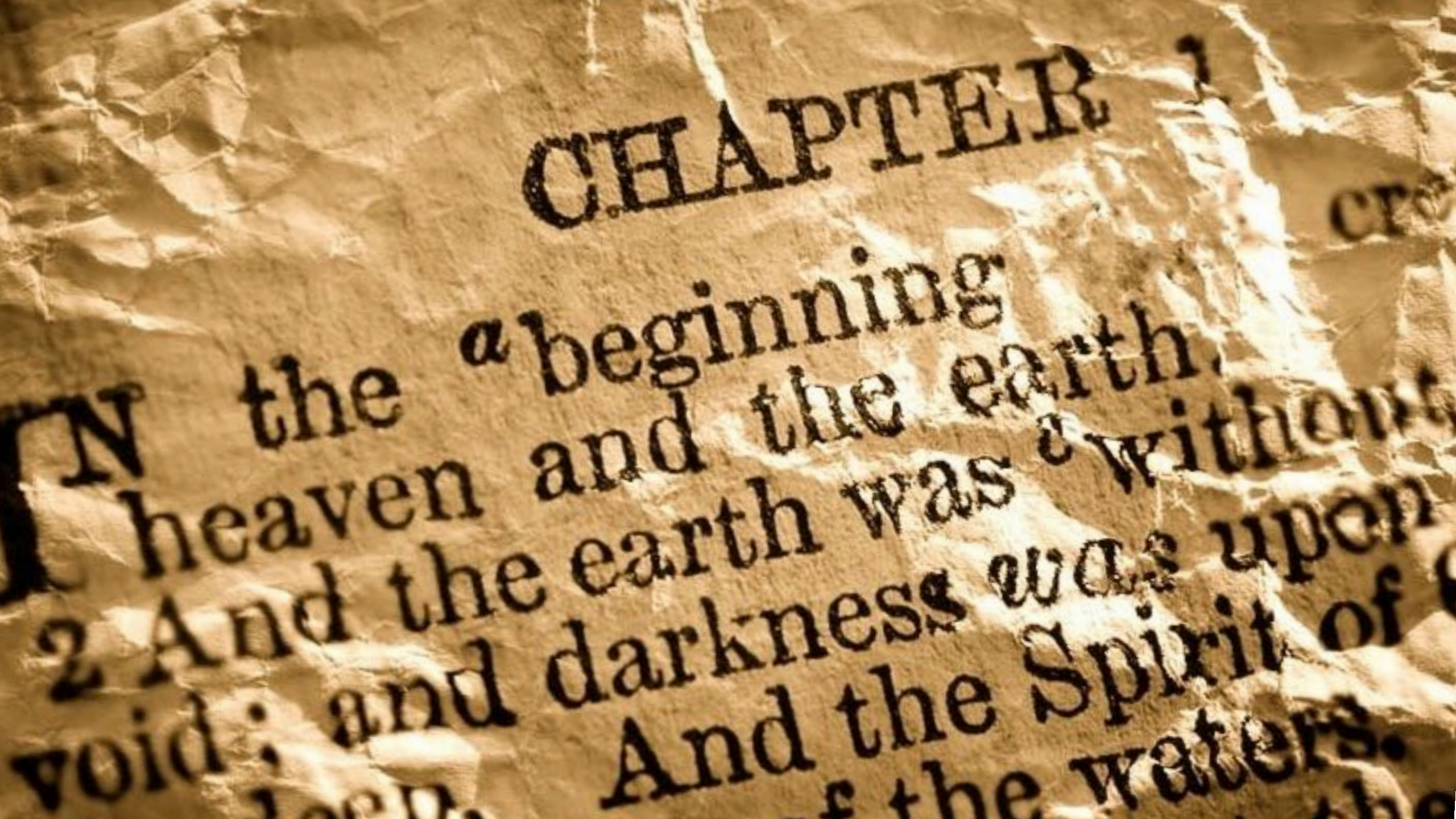
The future of the SOC…
or the SOC of the Future

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt
Chief Technologist Cybersecurity, DXC Technology
ISACA Hall of Fame

Past International Vice President, ISACA, Board of Directors
President, ISACA Barcelona Chapter
Executive Vice President, Quantum World Association
Privacy by Design Ambassador, Government of Ontario, Canada
IFGICT Fellow
ramses.gallego@dxc.com @ramsesgallego


the
future
is
now


X-MEN
DAYS OF FUTURE PAST


CHAPTER 1
N the beginning
heaven and the earth.
2 And the earth was without
void; and darkness was upon
And the Spirit of
of the waters.


concept


CHANGE
AHEAD


DIGITAL DISRUPTION


35
30%
20%
10%


MARVEL STUDIOS
IRON MAN

DXC and 7AI Partner to Deliver Revolutionary AI-Powered Security Operations Service

New agentic security service reduces operational costs through autonomous AI agents while delivering faster response times and scaling coverage

In 2025, 7AI's platform has saved security teams 224,000 analyst hours – equivalent to approximately 112 analyst years of work and $11.2 million

DXC TECHNOLOGY

Announcing New Strategic Partnership with 7AI

Team,

DXC was recently recognized in Gartner's Emerging Market Quadrant of the 2025 Gartner® Innovation Guide for Generative AI Consulting and Implementation Services. This is a testament to our work consulting with customers to harness the power of AI to drive business outcomes. In addition to that important work, we are also innovating to take advantage of AI for better operational outcomes in our IT and cyber services.

I'm excited to share that DXC has officially partnered with 7AI to launch a groundbreaking new service: the **DXC Agentic Security Operations Center (SOC).**

Together with 7AI, we are introduci… …urity solution that brings fully autonom… …managed security … means faster res… …, smarter threat detection and improved secur… for our cust… …while continuing to scale our capabilities like never before.

Mi… …er and our Global CISO organization were our customer zero test with 7AI, …e results were impressive:

- Reduction of more than 99 percent in analyst workload.
- Time to manage a single ticket improved by 68 percent.
- Investigation quality matched analyst performance more than 95 percent of the time.

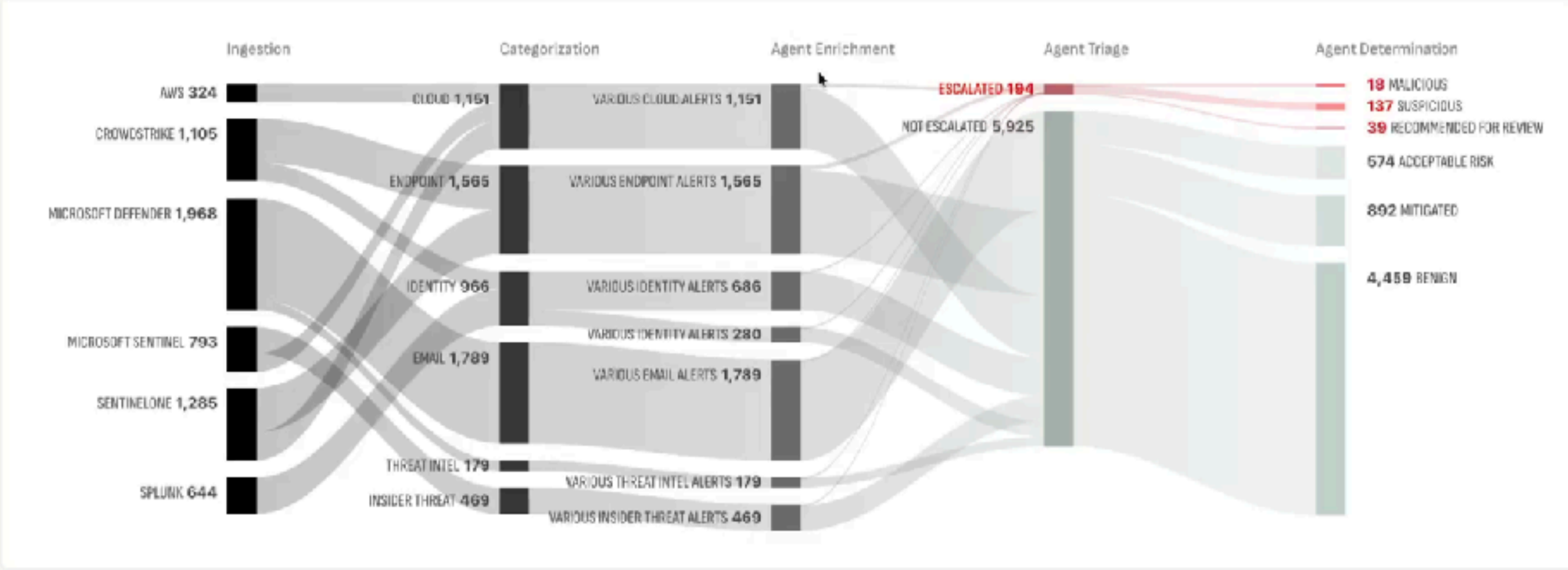
We now get to bring this capability to our managed services customers.

…partnership is more than just a new service launch. It is a bold s… …he future …security. Unlike our competitors – we are not just talk… …AI – we are implem…ing it for …roved outcomes. It reflects … …ment to innovation, to our customers and to staying … …apidly evolving market.

7AI

THE AGENTIC SECURITY REVOLUTION: HOW AI IS TRANSFORMING CYBERSECURITY

7AI Investigations last 7 days



ESCALATED ALERTS

194

NOT ESCALATED

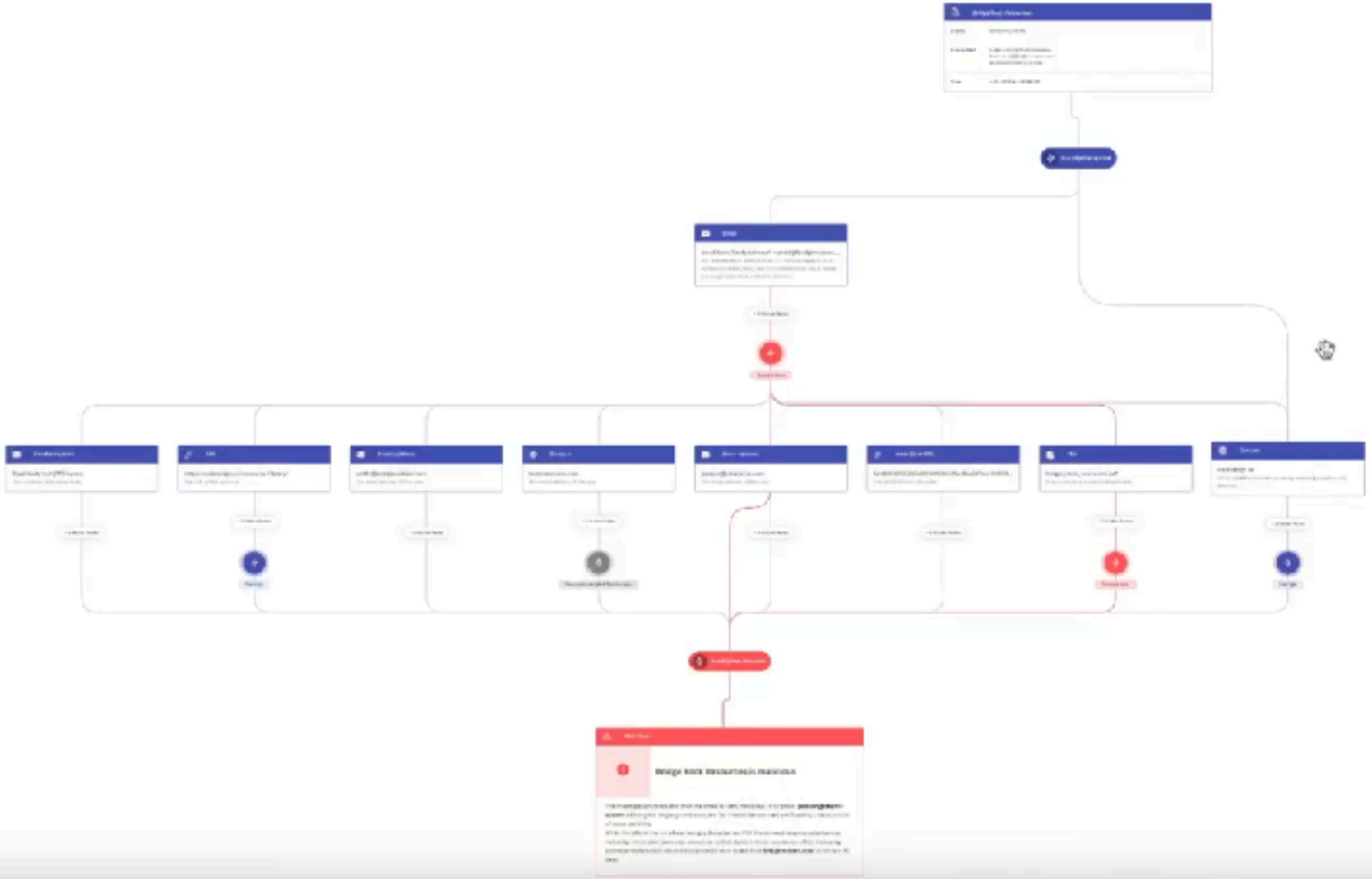
5,925

SOURCES

AWS	324	5.3%
CrowdStrike	1105	18.1%
Microsoft Defender	1968	32.2%

AGENT DETERMINATIONS

Malicious	18	<1%
Suspicious	137	2.2%
Recommended for review	39	<1%



Response


```
  "aggressive_language": {
    "reason": "The language used suggests a potential threat of limited account
access, which could be interpreted as coercive.",
    "severity": "medium"
  },
  "request_for_action": {
    "reason": "The email requests immediate action to verify the account,
implying urgency.",
    "severity": "high"
  },
  "request_for_information": {
    "reason": "The email indirectly requests personal account information in
order to verify the account.",
    "severity": "high"
  },
  "urgent_language": {
    "reason": "The phrase 'completed within the next 24 hours' evokes a sense
of urgency that could pressure the recipient.",
    "severity": "medium"
  }
}
implied_relationship:
The sender, Emily
                                                                    ources,
                  ionship with the recipient.
                  this relationship raises suspicion due to the email
                  y:
The email claims to be from 'Emily', an Account Manager at Bridge Rock
Resources, notifying the recipient, Jackson, of unusual activity detected on
```


The email claims to be from 'Emily', an Account Manager at Bridge Rock Resources, notifying the recipient, Jackson, of unusual activity detected on his account. The sender requests immediate verification of the account to avoid limited access. A secure link is provided for verification, along with an attachment detailing flagged activity. The sender emphasizes the need for prompt attention, suggesting a time-sensitive matter.

ail Analysis Agent ran Domain Whois

Email Analysis Agent ran Dom

Sort by Name

Show all artifacts

Domain

bridgerockres.com

Get Email Statistics By Email Domain
Found emails matching the domain bridgerockres.com in the last 90 days, their counts by Email Dir...

Domain Whois
whois query on the domain bridgerockres.com returned the following information: {'registrar': '', 'or...

Domain Reputation Check
The domain reputation is inconclusive

okami-ai.com

rockbridge.cc — Benign

Domain Categorization
No categorization information found for the domain

Domain Reputation Check
The domain is confirmed to be benign

Email

Email from "Emily Johnson" <emily@bridgerockres.com> to "Jackson Miller" <jackson@okami-ai.com> with subject Bridge Rock Resources — Malicious

Parse Email

Email address

emily@bridgerockres.com

Get Email Statistics By Email Address
Found emails matching the domain bridgerockres.com in the last 90 days, their counts by Email Dir...

jackson@okami-ai.com

User Profile Enrichment
No user profiles were found matching email

Find File Downloads By User
Did not find any additional emails sent from bridgerockres.com.

Email body text

vs. OTHER AI SOC TOOLS

Dropzone, Prophet, and other emerging vendors

WHEN THEY SAY:

"We're evaluating other AI analyst solutions. What makes 7AI different?"

OUR RESPONSE:

- **OTHER AI SOC TOOLS Limitation:** Point solutions focused on specific use cases without enterprise-grade deployment or transparency
- **DXC + 7AI's Advantage:** Enterprise-[illegible] security DNA, proven at scale, and full [illegible]
- **Bottom Line:** Other[illegible] offer AI experim[illegible] ready autonomous security operations

OTHER AI SOC TOOLS	7AI/DXC AGENTIC
Point solutions for specific security tasks	Comprehensive enterprise platform
Limited security industry heritage	Deep security and GI DNA
Expert mental or early-stage implementations	Proven in production processing millions of alerts
Black box AI with limited visibility	Full transparency into agent reasoning and decisions

vs. SOAR

Security Orchestration, Automation, and Response

WHEN THEY SAY:

"This sounds just like SOAR. We already have orchestration and playbooks."

OUR RESPONSE:

- **SOAR's Limitation:** Requires humans to investigate every alert and relies on rigid, predefined playbooks
- **7AI's Advantage:** Autonomous AI agents that investigate threats independently and adapt to novel attack patterns
- **Bottom Line:** SOAR orchestrates tools but still needs analysts. 7AI eliminates the analyst bottleneck entirely.

TRADITIONAL SOAR	7AI/DXC AGENTIC
Orchestrates predetermined playbooks	Dynamic reasoning without playbooks
Enriches data, analysts still perform investigations	Enriches data, completes full end-to-end investigations autonomously
Static workflows, manual updates required	Self-adapting to new attack techniques

All in one, SOAR is designed to orchestrate security tools and automate predefined workflows. While these capabilities improve efficiency, SOAR has one major limitation: it still requires humans to make decisions and act.

2

vs. TRADITIONAL MDR

Human-centric MDR/MSSP Services

WHEN THEY SAY:

"We already have an MDR provider. What makes DXC different?"

OUR RESPONSE:

- **Traditional MDR Limitation:** Still relies on human analysts to alert triage and investigation
- **DXC + 7AI's Advantage:** First MDR with fully autonomous AI agents handling analyst work
- **Bottom Line:** Other MDRs scale by adding analysts; our agents can scale to any environment automatically

SECURITY CO-PILOTS	7AI/DXC A[illegible]
[illegible] for investigation	[illegible] investigation
Inconsistent analysis quality	Consistent, comprehensive
Limited by analyst availability and location	24/7 autonomous, expert-level coverage
High false positive rates consume resources	AI agents eliminate false positives

MDR services delivered by DXC and 7AI deliver faster, more consistent results using a combination of AI agents and DXC security expertise.

vs. CO-PILOTS

Tools designed to give people better answers.

WHEN THEY SAY:

"We're looking at Microsoft Copilot or other AI assistants for security."

OUR RESPONSE:

- **Co-Pilot's Limitation:** Assists human analysts but doesn't replace their work—still requires human investigation
- **7AI's Advantage:** Fully autonomous agents that work 24/7 without human intervention
- **Bottom Line:** Co-pilots help analysts work faster. AI agents do the work.

SECURITY [illegible]-PILOTS	7AI/DXC AGENTIC
AI provides insights [illegible] for human analysts	Autonomous AI agents replacing manual work
Accelerates human decision-making	Makes decisions independently
Reduces time to insight	Eliminates time to action

Co-pilots were designed to make people faster at doing manual, repetitive work. Agentic security eliminates the work entirely, letting people focus on more strategic, high-value security initiatives.

4

vs. HYPERAUTOMATION

WHEN THEY SAY:

"We're looking at hyperautomation platforms like Torq that claim 90% automation."

OUR RESPONSE:

- **Hyperautomation's Limitation:** Still workflow-based automation requiring playbook creation and maintenance, even with AI assistance
- **7AI's Advantage:** Truly autonomous agents that investigate and reason without predefined workflows or playbooks
- **Bottom Line:** Hyperautomation automates workflows faster. 7AI eliminates the need for workflows entirely

HYPERAUTOMATION	7AI/DXC AGENTIC
No-code/low-code workflow builders with AI	Self-directed AI agents with dynamic reasoning
Still requires building and maintaining automations	Enriches data, completes full end-to-end investigations autonomously
"Agentic AI" within predefined workflow bounds	True autonomous agents operating without workflows

Why build another workflow when you can deploy agents that reason and adapt?

5

Best Practice Security Architecture Framework

Threat Protection | Information Protection | Other | IT-GRC / Prepare | Detection and Response

Governance, Risk and Compliance
- Risk Dashboard
- 3rd Party Risk Mgmt.
- Regulatory Compliance
- Risk Statistics

Identity and Access Management
- Single Sign-On
- Multi-Factor Authentication
- Privileged Access Management
- Identity Management

Internet of Things
- Behavioural Security Engine
- USB Sanitisation

Security Operations Centre
- Security Monitoring
- Security Log Collection
- Threat Investigation & Response
- Malware Analysis
- Event Ticketing
- Packet Capture & Forensics
- Workflow Automation
- Integration Platform
- Threat Intelligence Feed

Technical Services
- Premium Support
- Value Realisation

End-User Devices
- Endpoint Protection
- Active Directory Defence
- Detection & Response
- APT & Sandboxing
- System Hardening
- Deception
- Endpoint Device & Patch Mgmt
- Browser Isolation
- Endpoint Encryption
- Data Loss Prevention
- Mobile Threat Protection
- Compliance Mgmt

Content and Collaboration
- On-Prem Email Protection
- Direct-to-Net Email Protection
- Direct-to-Net Detection & Response
- On-Prem Content & Malware Analysis
- Secure Cloud Adoption
- Collaboration Platform Security
- Messaging Platform Security
- Email Isolation
- File, Email & Cloud Encryption
- Data Loss Prevention

Infrastructure
- On-Prem Web Protection
- Network Access Control
- Direct-to-Net Web Protection
- DNS Filtering
- Detection & Response
- Firewalls
- Content & Malware Analysis
- Intrusion Detection
- PKI
- DDoS Prevention
- Packet Capture & Forensics
- Standards & Vulnerability Mgmt.
- IT Systems & Patch Mgmt.
- Network Monitoring & Optimisation
- Encrypted Traffic Mgmt.
- Data Loss Prevention

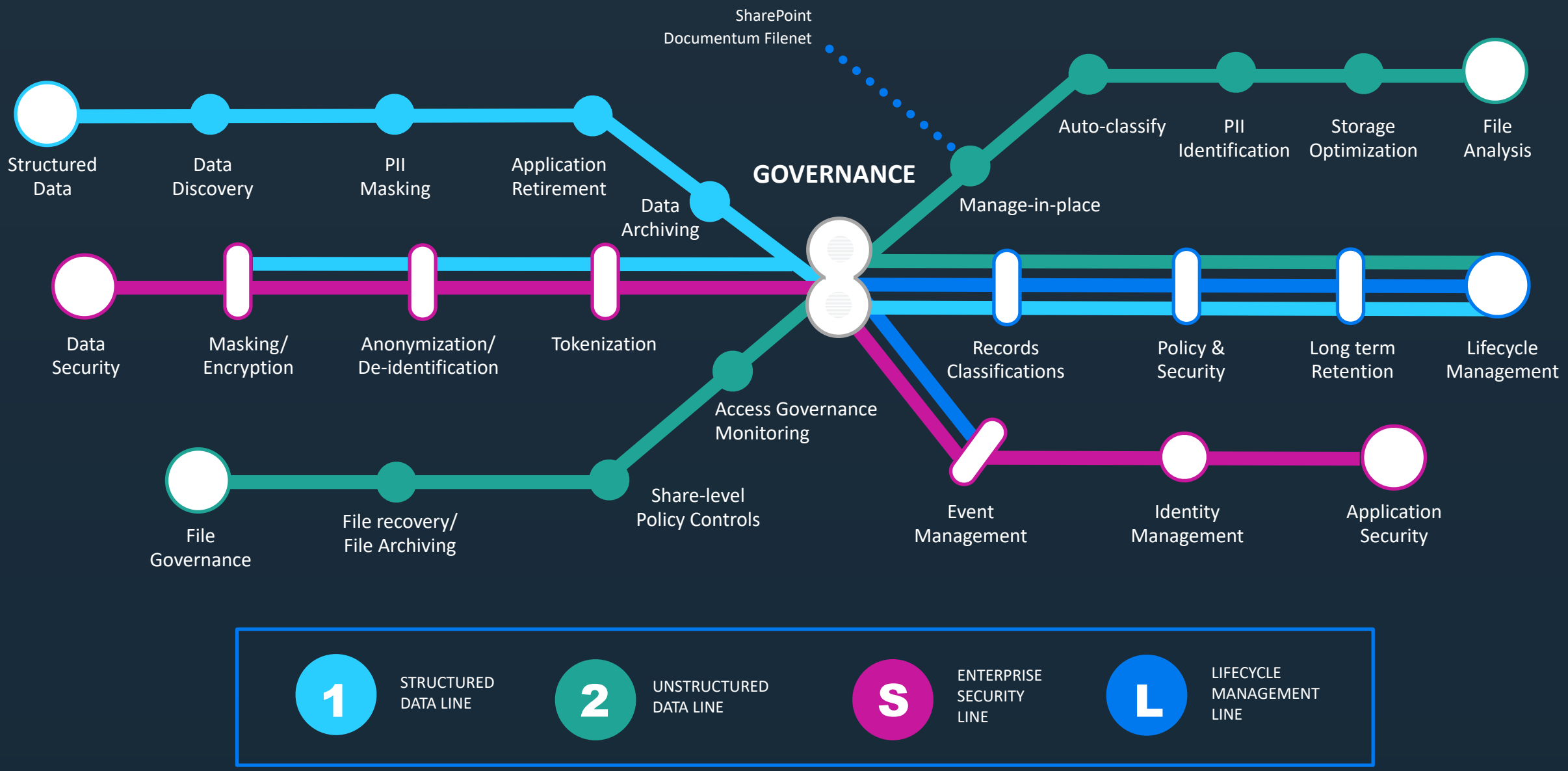
DXC TECHNOLOGY

Compute, Storage & Applications
- Cloud Security Posture
- Workload Protection
- Cloud Storage Security
- WAF & Reverse Proxy
- Secure Cloud Adoption
- Server Malware Protection
- Static & Dynamic Code Analysis
- System Hardening
- Malware for Storage
- DLP for Storage
- DLP for Cloud
- Cloud App Anti-Malware

Data
- Data Encryption
- Data Loss Prevention
- Data Classification
- User Entity Behaviour Analytics

Services
- Incident Response
- Actor Intelligence
- Phishing Readiness
- Security Awareness Training
- Capability Education
- Threat Research
- Security Monitoring


EVERYTHING
EVERYWHERE
ALL AT ONCE


SharePoint
Documentum Filenet
GOVERNANCE
Structured Data
Data Discovery
PII Masking
Application Retirement
Data Archiving
Auto-classify
PII Identification
Storage Optimization
File Analysis
Manage-in-place
Data Security
Masking/ Encryption
Anonymization/ De-identification
Tokenization
Records Classifications
Policy & Security
Long term Retention
Lifecycle Management
Access Governance Monitoring
File Governance
File recovery/ File Archiving
Share-level Policy Controls
Event Management
Identity Management
Application Security
1
STRUCTURED DATA LINE
2
UNSTRUCTURED DATA LINE
S
ENTERPRISE SECURITY LINE
L
LIFECYCLE MANAGEMENT LINE

Data Protection

GVB

User Behavioral Analytics

AI-driven SecOps

Privacy Enhancing

Risk Findings

Structured Data

Data Discovery

Test Data Management

Application Retirement

Data Archiving

Risk Analytics

Classification

PI/ PII Detection

Data Discovery

Unstructured Data

External Activities

OCR/ Audio/ Video

Metadata Enrichment

External Action
- Redact
- Encrypt
- Hold

Cloud Analytics Workloads

Data Trust

Mask

Encrypt

Tokenize

Data Protection

Zero Trust

Access Monitoring & Reporting

Data Access Governance

Attestation

Rights Remediation

Defensible Disposition

Long term Retention

Policy & Security

Lifecycle Management

Privacy Preserving

Identity & Access Management

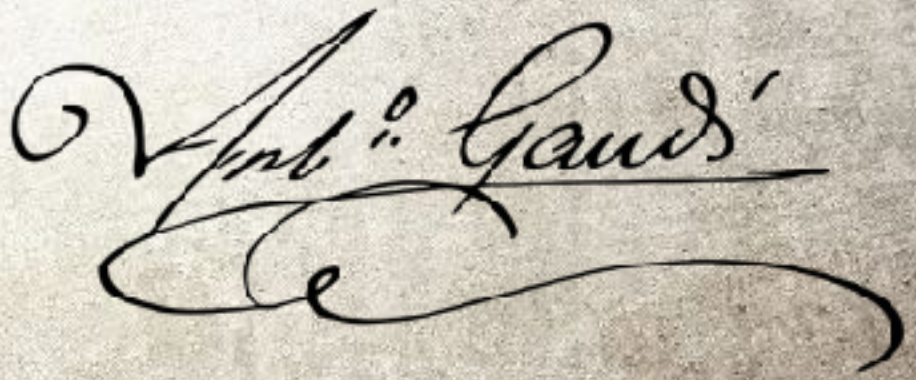
1 STRUCTURED DATA LINE

2 UNSTRUCTURED DATA LINE

P PROTECTION LINE

L DATA LIFECYCLE LINE

‘…originality consists on returning to the origin’



THANK YOU

The Future of the SOC... or the SOC of the Future

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt
Chief Technologist Cybersecurity, DXC Technology
ISACA Hall of Fame

Past International Vice President, ISACA, Board of Directors
President, ISACA Barcelona Chapter
Executive Vice President, Quantum World Association
Privacy by Design Ambassador, Government of Ontario, Canada
IFGICT Fellow
ramses.gallego@dxc.com @ramsesgallego