WORKFORCE CYBER INTELLIGENCE & SECURITY

DTEX InTERCEPT

Next-Generation Insider Risk Management

Chris Harris, SVP Public Sector
JD DuHaime, VP Public Sector - DOD
Andy London, Sr Dir Engineering
Mike Rider, Sr Solution Architect

ABOUT DTEX

THE GLOBAL LEADER IN INSIDER RISK MGT (IRM)

US Based in San Jose, Ca

Relevant References

- DISA Rapid Innovation Fund 2016 → CNSSD-504
- Services Australia
- ABS
- DSTG
- VIC & SA Govt
- Johns Hopkins University Applied Physics Laboratory (JHU APL)
- DHS
- Federal Trade Commission (FTC)
- Brookhaven National Laboratory, DOE
- MoD Netherlands
- Critical Infrastructure:
  - BHP / NBN / NAB / Fannie Mae / Citi / Capital One / Blackrock / NASDAQ / NextEra / Duke Energy / United Airlines

Executive References

- Marshall Heilman (17yr Mandiant Exec, now DTEX CEO)
- Bob Lentz (DTEX board member & former CISO, US DoD)
- Derek Smith (DTEX Shareholder & Founder of Raytheon SureView/Innerview solution)

CapitalG

Strategic Partnerships & Integrations

MITRE | INSIDE-R PROTECT™ IN PARTNERSHIP WITH DTEX

splunk> aws

Australian Government
Department of Defence
Defence Science and Technology Group

CROWDSTRIKE Microsoft Deloitte. FIVECAST

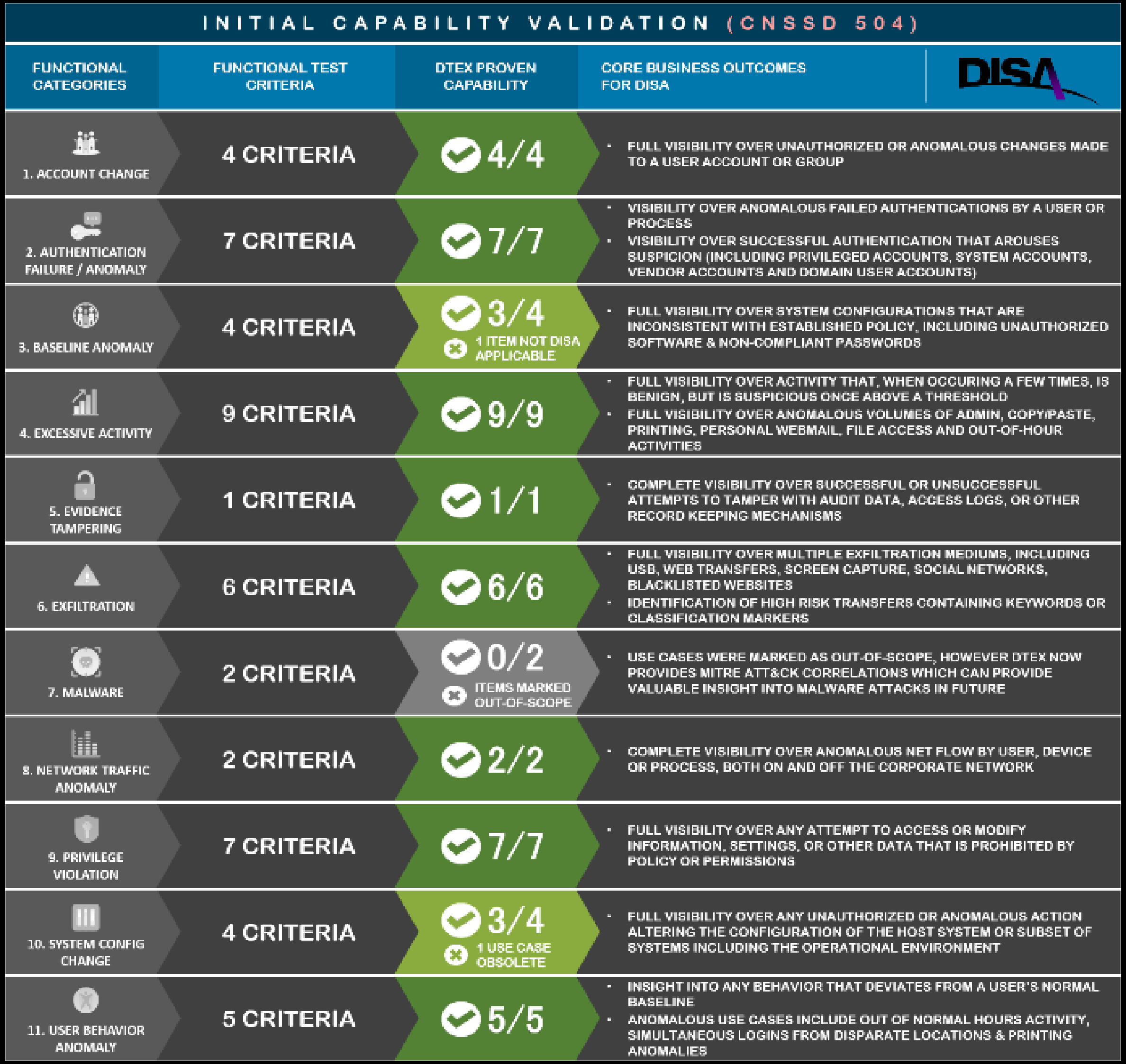
DTEX InT RESEARCH & DEVELOPMENT REFERENCE #1:

DISA Insider Threat & Credential Misuse

2017 - 2019

- 2 Year Rapid Innovation Fund (RIF) to research and develop a solution to automate:
  - The detection of lateral movement
  - Flag unusual use of legitimate credentials
  - Alert on situations of multiple, simultaneous login attempts and other anomalous user behaviors
- Interim ATO approved and demonstrated enterprise scalability and no impact to DISA devices
  - Near-zero performance impact to endpoint/network (<0.5% CPU, 3 - 4MB per Endpoint per Day)
- DISA recommendations become basis for new InTERCEPT Focused Observation module – released 2021

  (includes screen recording, keystroke logging → full CNSSD 504 requirements met)



INITIAL CAPABILITY VALIDATION (CNSSD 504)

FUNCTIONAL CATEGORIES	FUNCTIONAL TEST CRITERIA	DTEX PROVEN CAPABILITY	CORE BUSINESS OUTCOMES FOR DISA
1. ACCOUNT CHANGE	4 CRITERIA	✓ 4/4	• FULL VISIBILITY OVER UNAUTHORIZED OR ANOMALOUS CHANGES MADE TO A USER ACCOUNT OR GROUP
2. AUTHENTICATION FAILURE / ANOMALY	7 CRITERIA	✓ 7/7	• VISIBILITY OVER ANOMALOUS FAILED AUTHENTICATIONS BY A USER OR PROCESS • VISIBILITY OVER SUCCESSFUL AUTHENTICATION THAT AROUSES SUSPICION (INCLUDING PRIVILEGED ACCOUNTS, SYSTEM ACCOUNTS, VENDOR ACCOUNTS AND DOMAIN USER ACCOUNTS)
3. BASELINE ANOMALY	4 CRITERIA	✓ 3/4 ☒ 1 ITEM NOT DISA APPLICABLE	• FULL VISIBILITY OVER SYSTEM CONFIGURATIONS THAT ARE INCONSISTENT WITH ESTABLISHED POLICY, INCLUDING UNAUTHORIZED SOFTWARE & NON-COMPLIANT PASSWORDS
4. EXCESSIVE ACTIVITY	9 CRITERIA	✓ 9/9	• FULL VISIBILITY OVER ACTIVITY THAT, WHEN OCCURING A FEW TIMES, IS BENIGN, BUT IS SUSPICIOUS ONCE ABOVE A THRESHOLD • FULL VISIBILITY OVER ANOMALOUS VOLUMES OF ADMIN, COPY/PASTE, PRINTING, PERSONAL WEBMAIL, FILE ACCESS AND OUT-OF-HOUR ACTIVITIES
5. EVIDENCE TAMPERING	1 CRITERIA	✓ 1/1	• COMPLETE VISIBILITY OVER SUCCESSFUL OR UNSUCCESSFUL ATTEMPTS TO TAMPER WITH AUDIT DATA, ACCESS LOGS, OR OTHER RECORD KEEPING MECHANISMS
6. EXFILTRATION	6 CRITERIA	✓ 6/6	• FULL VISIBILITY OVER MULTIPLE EXFILTRATION MEDIUMS, INCLUDING USB, WEB TRANSFERS, SCREEN CAPTURE, SOCIAL NETWORKS, BLACKLISTED WEBSITES • IDENTIFICATION OF HIGH RISK TRANSFERS CONTAINING KEYWORDS OR CLASSIFICATION MARKERS
7. MALWARE	2 CRITERIA	✓ 0/2 ☒ ITEMS MARKED OUT-OF-SCOPE	• USE CASES WERE MARKED AS OUT-OF-SCOPE, HOWEVER DTEX NOW PROVIDES MITRE ATT&CK CORRELATIONS WHICH CAN PROVIDE VALUABLE INSIGHT INTO MALWARE ATTACKS IN FUTURE
8. NETWORK TRAFFIC ANOMALY	2 CRITERIA	✓ 2/2	• COMPLETE VISIBILITY OVER ANOMALOUS NET FLOW BY USER, DEVICE OR PROCESS, BOTH ON AND OFF THE CORPORATE NETWORK
9. PRIVILEGE VIOLATION	7 CRITERIA	✓ 7/7	• FULL VISIBILITY OVER ANY ATTEMPT TO ACCESS OR MODIFY INFORMATION, SETTINGS, OR OTHER DATA THAT IS PROHIBITED BY POLICY OR PERMISSIONS
10. SYSTEM CONFIG CHANGE	4 CRITERIA	✓ 3/4 ☒ 1 USE CASE OBSOLETE	• FULL VISIBILITY OVER ANY UNAUTHORIZED OR ANOMALOUS ACTION ALTERING THE CONFIGURATION OF THE HOST SYSTEM OR SUBSET OF SYSTEMS INCLUDING THE OPERATIONAL ENVIRONMENT
11. USER BEHAVIOR ANOMALY	5 CRITERIA	✓ 5/5	• INSIGHT INTO ANY BEHAVIOR THAT DEVIATES FROM A USER'S NORMAL BASELINE • ANOMALOUS USE CASES INCLUDE OUT OF NORMAL HOURS ACTIVITY, SIMULTANEOUS LOGINS FROM DISPARATE LOCATIONS & PRINTING ANOMALIES

NITTF EXECUTIVE ORDER 13587, DISA STIG, AND NIST FRAMEWORK

- Executive Order 13587 directs the US Government agencies to establish, implement, monitor and report on the effectiveness of insider threat programs to protect classified national security information (as defined in Executive Order 13526; hereinafter classified information), and requires the development of an executive branch program for the deterrence, detection, and mitigation of insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure.

- DTEX adheres to recommended best practices identified within government guidelines such as **US Government Configuration Baseline** and associated **DISA Security Technical Implementation Guides**

- All ports, interfaces, and services are documented and all ports, interfaces, and services that require authentication meet the requirements of **NIST SP 800-63** or other equivalent applicable standard.

THE COST OF DOING NOTHING

$15.38M

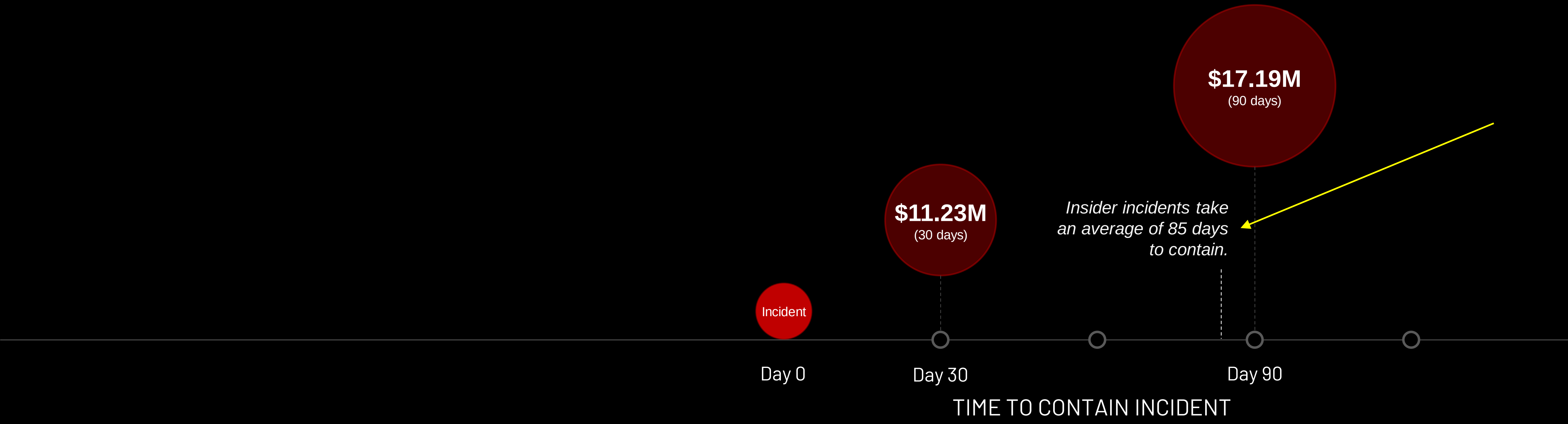
average annual cost of insider-led cyber incidents

(2022 Ponemon Cost of an Insider Threat Report)

85%

of breaches involved human interaction

(Verizon 2021 Data Breach Investigation)



Incident

$11.23M
(30 days)

$17.19M
(90 days)

Insider incidents take an average of 85 days to contain.

Day 0

Day 30

Day 90

TIME TO CONTAIN INCIDENT

THE BENEFITS OF AN INSIDER RISK PROGRAM

91%

fewer Insider Threat incidents

(2022 DTEX Insider Risk Report)

validated in the largest data driven Insider Threat study ever conducted

DTEX InTERCEPT

LEFT OF BOOM

PROACTIVE DETECTION AND PREVENTION OF INSIDER THREATS

THE COST OF DOING NOTHING

$15.38M

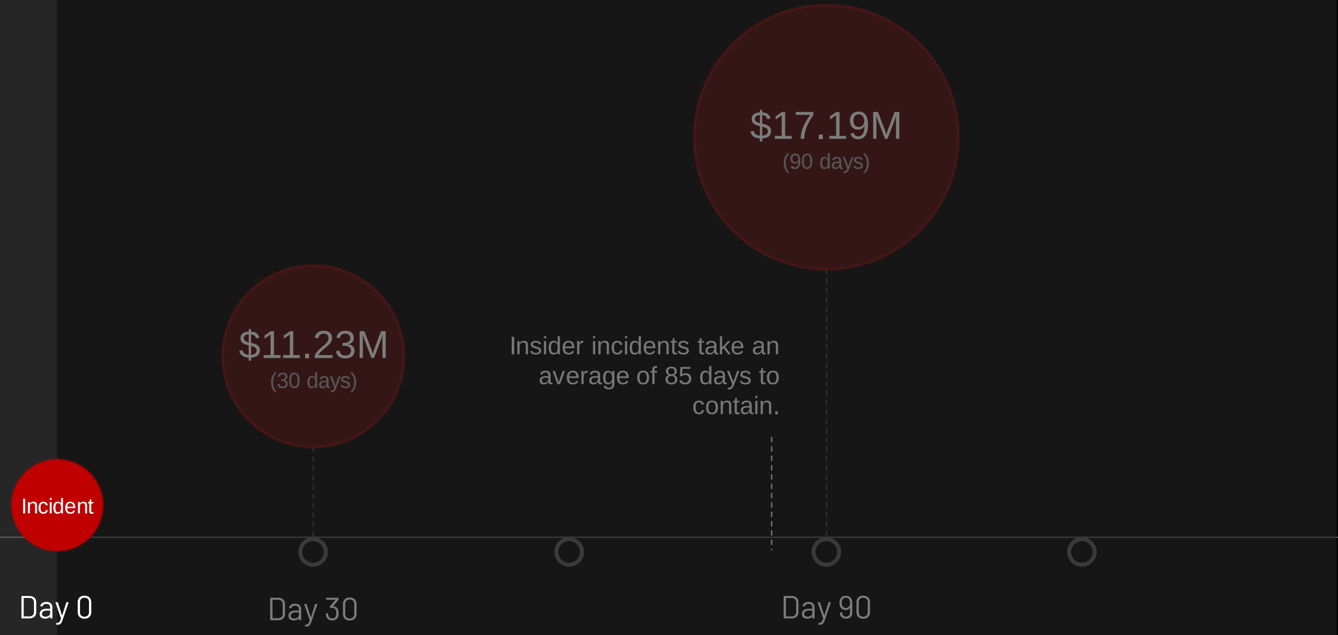
average annual cost of insider-led cyber incidents

(2022 Ponemon Cost of an Insider Threat Report)

85%

of breaches involved an insider

(Verizon 2021 Data Breach Investigation)



Insider incidents take an average of 85 days to contain.

TIME TO CONTAIN INCIDENT

WHAT'S MISSING?

NEXT-GEN AV

MALWARE FOCUS

1. EPP (AV)
2. EDR
3. IOC's
4. MITRE ATT&CK

CROWDSTRIKE Microsoft

?

NEXT-GEN SIEM

DATA FOCUS

1. SIEM
2. SOAR
3. CASE MGMT
4. APP ECOSYSTEM

splunk> exabeam

NEXT-GEN FIREWALL

NETWORK FOCUS

1. IDS / IPS
2. NDR
3. WAF
4. FIREWALL

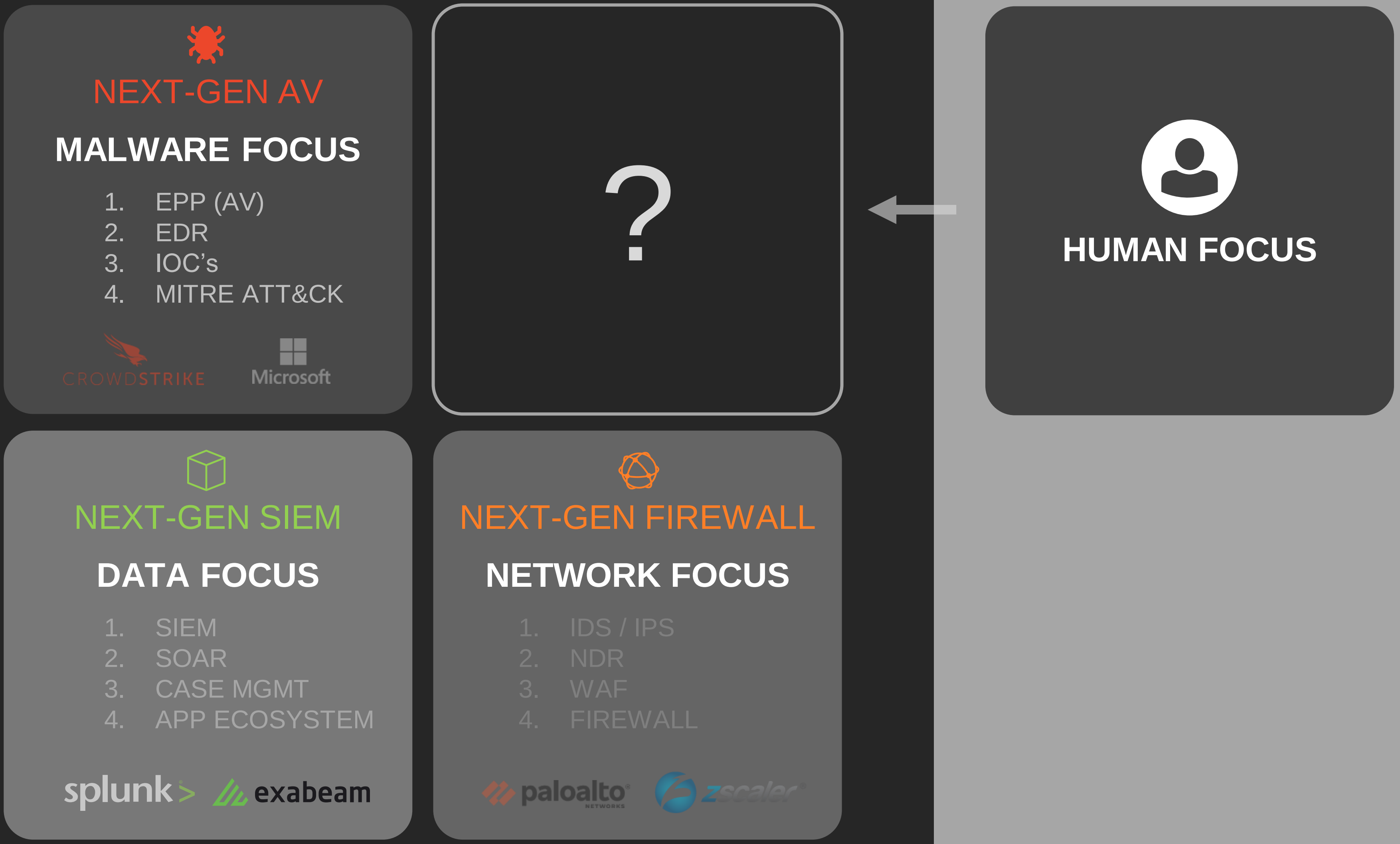
paloalto NETWORKS zscaler

**logos shown are key DTEX integration partners*

DTEX

WHAT'S MISSING?

WHAT IS NEEDED?



NEXT-GEN AV

MALWARE FOCUS

1. EPP (AV)
2. EDR
3. IOC's
4. MITRE ATT&CK

HUMAN FOCUS

NEXT-GEN SIEM

DATA FOCUS

1. SIEM
2. SOAR
3. CASE MGMT
4. APP ECOSYSTEM

NEXT-GEN FIREWALL

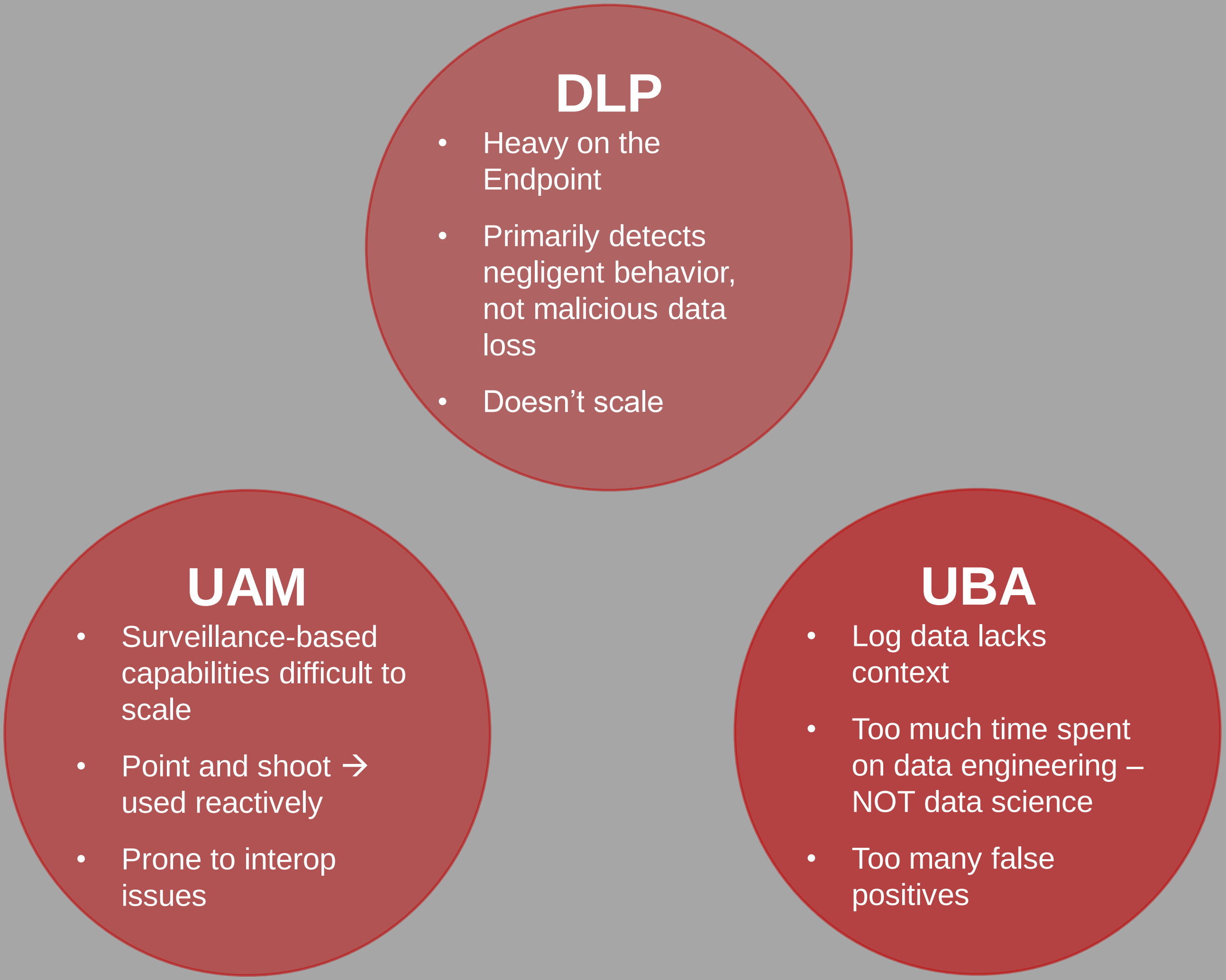
NETWORK FOCUS

1. IDS / IPS
2. NDR
3. WAF
4. FIREWALL

**logos shown are key DTEX integration partners*

WHAT WENT WRONG?

HUMAN FOCUS



DLP

- Heavy on the Endpoint
- Primarily detects negligent behavior, not malicious data loss
- Doesn’t scale

UAM

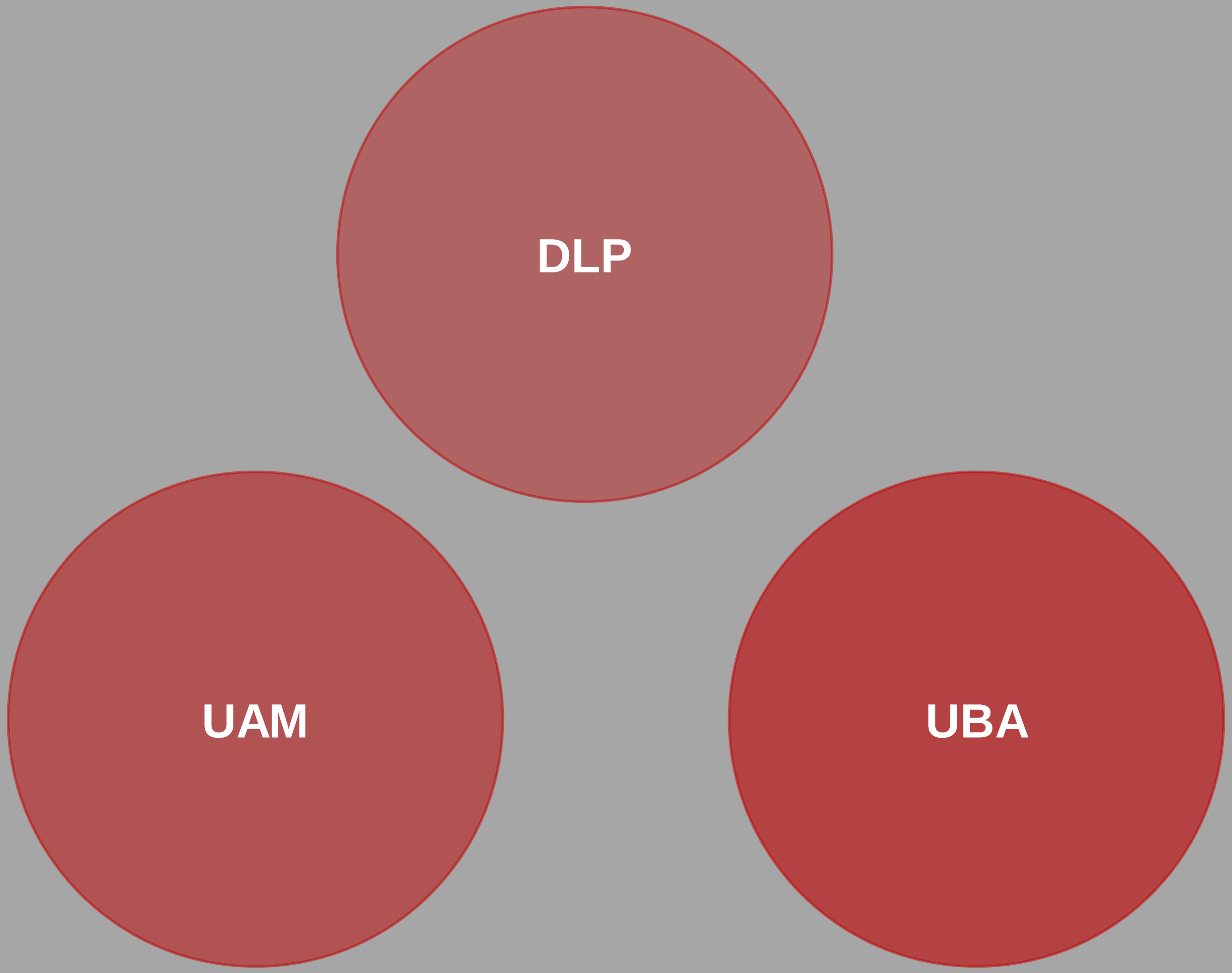
- Surveillance-based capabilities difficult to scale
- Point and shoot → used reactively
- Prone to interop issues

UBA

- Log data lacks context
- Too much time spent on data engineering – NOT data science
- Too many false positives

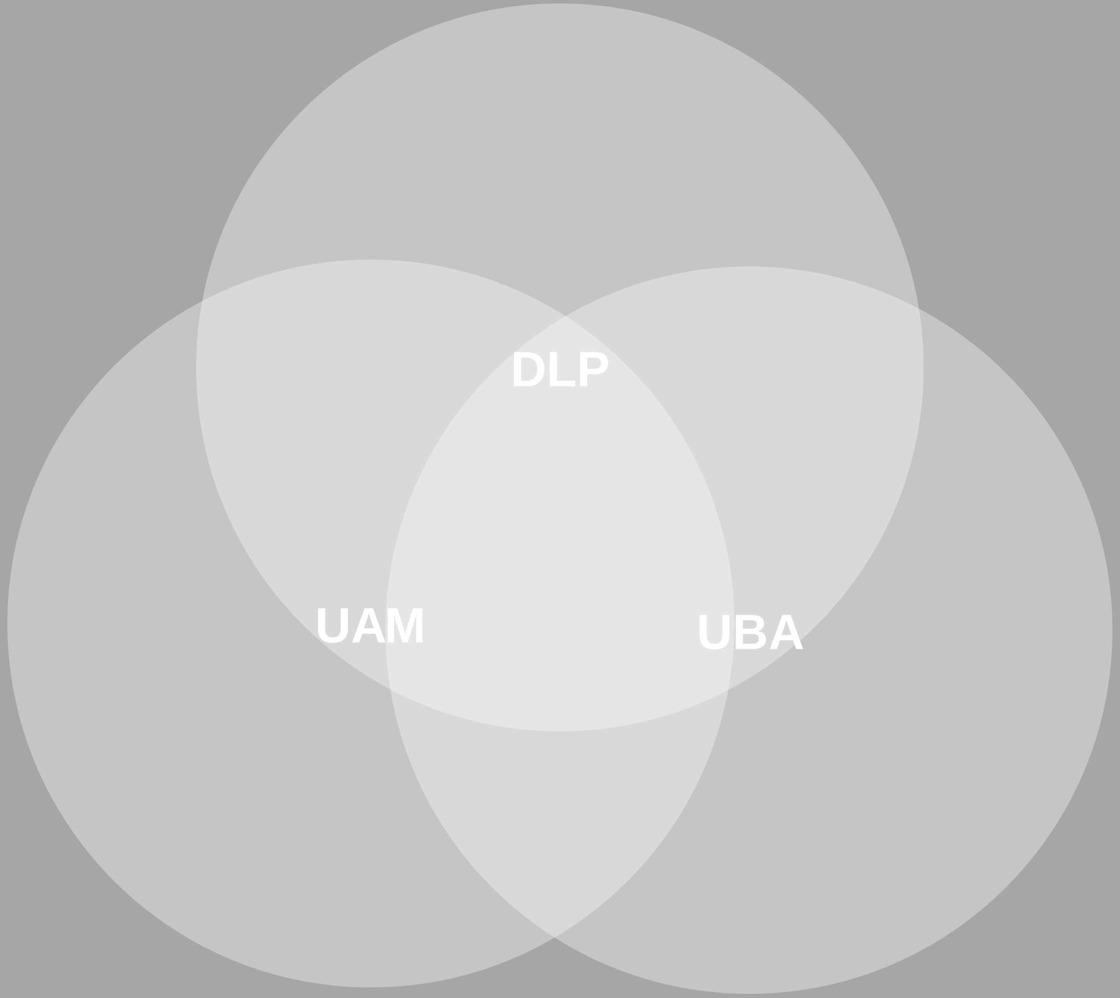
THE CONVERGENCE

HUMAN FOCUS



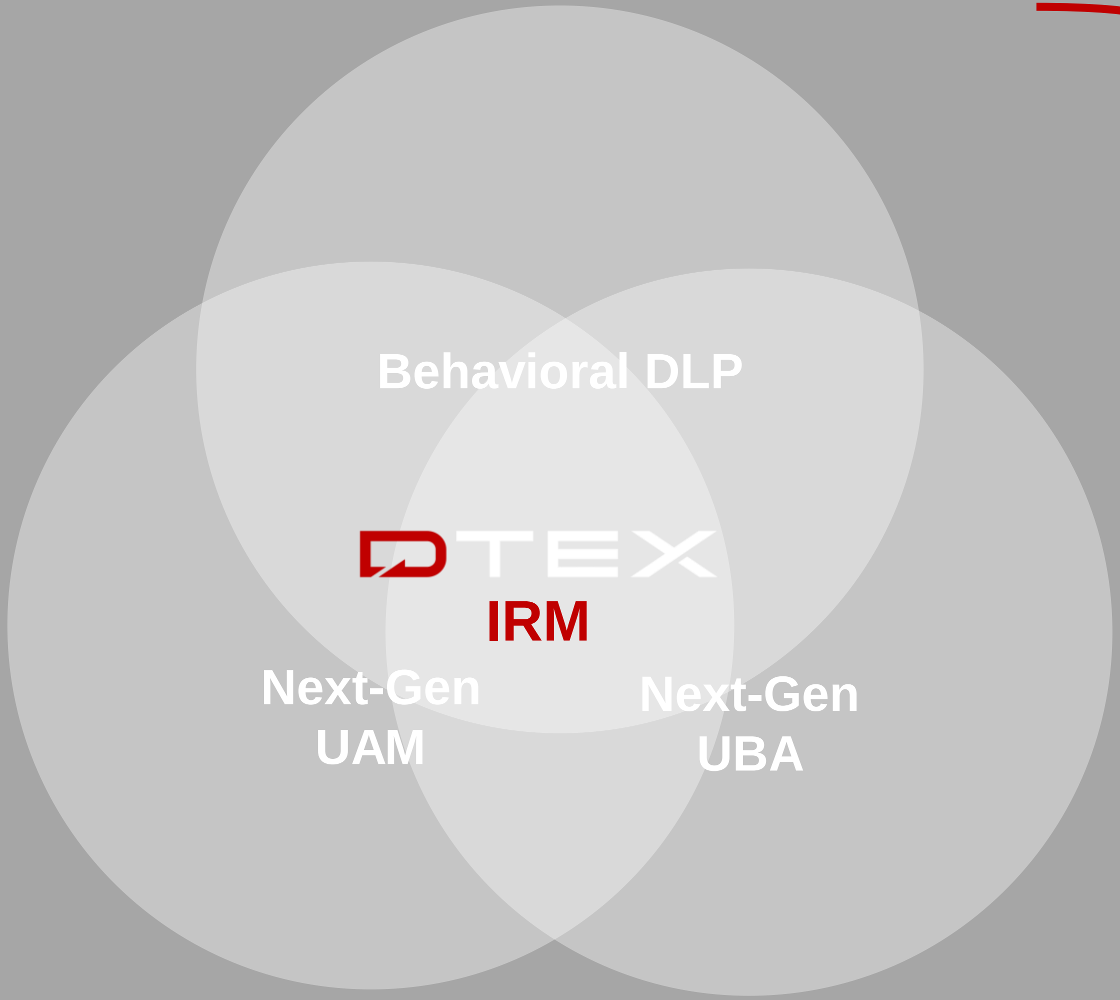
THE CONVERGENCE

HUMAN FOCUS



THE CONVERGENCE

HUMAN FOCUS



Behavioral DLP

DTEX IRM

Next-Gen UAM

Next-Gen UBA

Gartner®

Insider Risk Management (IRM)

NEXT-GEN INSIDER

HUMAN FOCUS

1. UAM
2. DLP
3. UBA
4. FORENSICS

COMPLETING THE PICTURE

NEXT-GEN AV

MALWARE FOCUS

1. EPP (AV)
2. EDR
3. IOC's
4. MITRE ATT&CK

CROWDSTRIKE Microsoft

NEXT-GEN INSIDER

HUMAN FOCUS

1. UAM
2. DLP
3. UBA
4. FORENSICS

DTEX

NEXT-GEN SIEM

DATA FOCUS

1. SIEM
2. SOAR
3. CASE MGMT
4. APP ECOSYSTEM

splunk> exabeam

NEXT-GEN FIREWALL

NETWORK FOCUS

1. IDS / IPS
2. NDR
3. WAF
4. FIREWALL

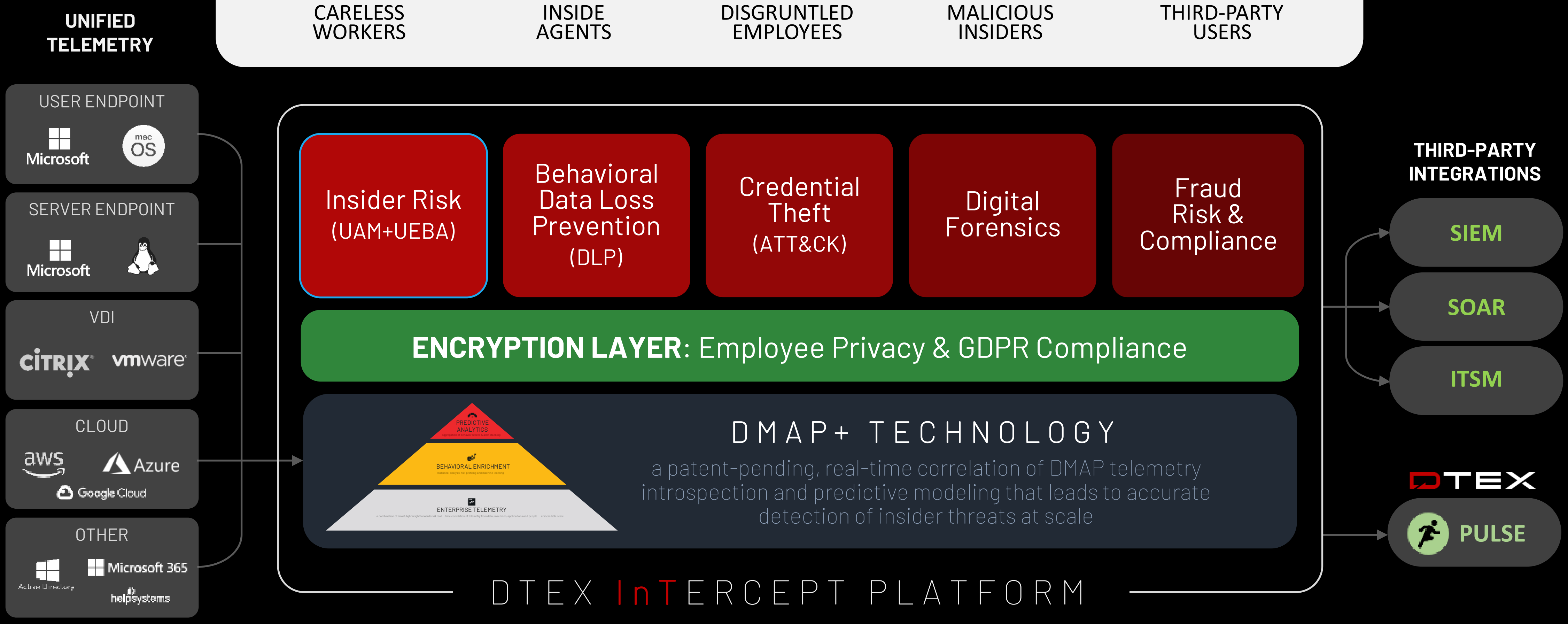
paloalto NETWORKS zscaler

**logos shown are key DTEX integration partners*

DTEX InTERCEPT PLATFORM

Most Common Types of Insider Threats

- CARELESS WORKERS
- INSIDE AGENTS
- DISGRUNTLED EMPLOYEES
- MALICIOUS INSIDERS
- THIRD-PARTY USERS



UNIFIED TELEMETRY

USER ENDPOINT: Microsoft, macOS

SERVER ENDPOINT: Microsoft

VDI: citrix, vmware

CLOUD: aws, Azure, Google Cloud

OTHER: Active Directory, Microsoft 365, helpsystems

Insider Risk (UAM+UEBA)

Behavioral Data Loss Prevention (DLP)

Credential Theft (ATT&CK)

Digital Forensics

Fraud Risk & Compliance

ENCRYPTION LAYER: Employee Privacy & GDPR Compliance

DMAP+ TECHNOLOGY

a patent-pending, real-time correlation of DMAP telemetry introspection and predictive modeling that leads to accurate detection of insider threats at scale

PREDICTIVE ANALYTICS
aggregation of behavior scores & alert stacking
BEHAVIORAL ENRICHMENT
statistical analysis, risk profiling and machine learning
ENTERPRISE TELEMETRY
a combination of smart, lightweight forwarders & real -time correlation of telemetry from data, machines, applications and people at incredible scale

DTEX InTERCEPT PLATFORM

THIRD-PARTY INTEGRATIONS

- SIEM
- SOAR
- ITSM

DTEX PULSE

ZERO IMPACT →
5MB PER DAY
(PER ENDPOINT)

Demonstration

DTEX InTERCEPT

VERTICAL: FED

Agency of DHS

Pain: UAM/UBA

DTEX Systems

www.dtexsystems.com

Competition:

Forcepoint (DHS Incumbent)

1

Background

Department of Homeland Security (DHS) requires all DHS Components to procure and deploy a UAM/UBA capability on all DHS networks by Executive Order 13587

This agency had a desire to consolidate various endpoint log data sources into a single data telemetry, which could not be achieved with the current solution.

Goal: Integration with Existing Tools – to improve performance of existing security tools in building a stronger security eco-system and procure Next Gen Technology

2

Approach

Developed an internal champion; educated agency on value of DTEX leveraging MITRE Partnership; dwelled on Forcepoint pain points

Built confidence and established a relationship with the right partner, GuidePoint

Proved value and received technical win via POV

Validated Sales Process with technical results – providing technical resources and foocused work sessions tailored to each team (SOC, IRM, EP, Data Protection, Analytics)

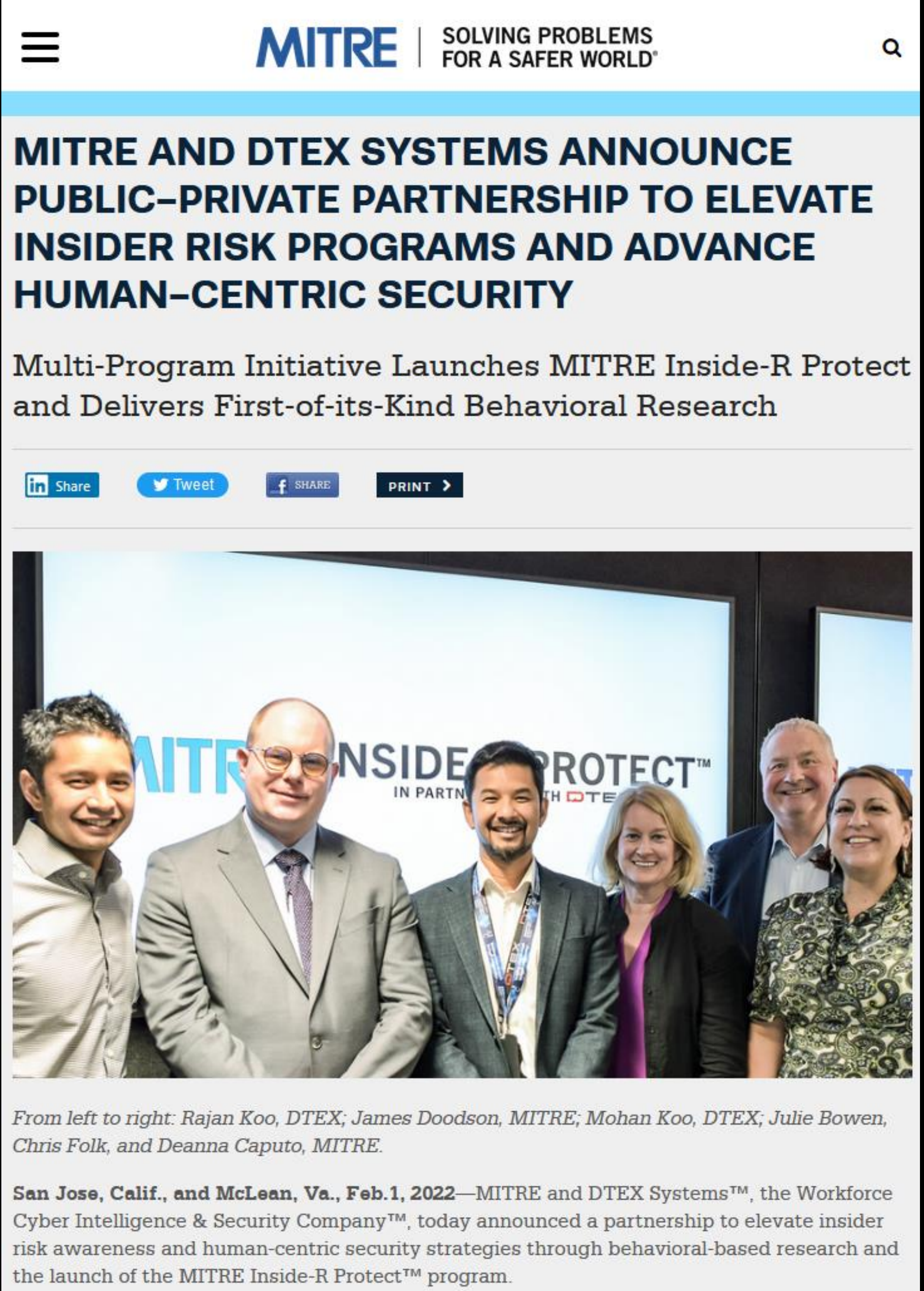
3

Outcomes

Helped agency meet their UAM/UBA requirements in a single platform

Agency saw improved performance, consolidation to Insider Risk/UAM, Forensics, User Behavior Data Sensitivity, User Behavior Privacy all to support offices within agency to include several offices. This agencies current tools lacked the ability to detect malicious and/or anomalous activity typically indicative of insider threats as required by the Executive Order

Opportunity for future growth here, winning over such a large agency provides an opportunity into further FED business and has a ripple effect on our commercial side of our business



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

MITRE AND DTEX SYSTEMS ANNOUNCE PUBLIC–PRIVATE PARTNERSHIP TO ELEVATE INSIDER RISK PROGRAMS AND ADVANCE HUMAN–CENTRIC SECURITY

Multi-Program Initiative Launches MITRE Inside-R Protect and Delivers First-of-its-Kind Behavioral Research

From left to right: Rajan Koo, DTEX; James Doodson, MITRE; Mohan Koo, DTEX; Julie Bowen, Chris Folk, and Deanna Caputo, MITRE.

San Jose, Calif., and McLean, Va., Feb.1, 2022—MITRE and DTEX Systems™, the Workforce Cyber Intelligence & Security Company™, today announced a partnership to elevate insider risk awareness and human-centric security strategies through behavioral-based research and the launch of the MITRE Inside-R Protect™ program.

MITRE | INSIDE-R PROTECT™ IN PARTNERSHIP WITH DTEX

Launched in January 2022

- ❖ New indicators for Super Malicious Insiders
- ❖ Not-for-profit Service Offering
- ❖ MITRE Applied Research Centre in ADL
- ❖ MITRE ‘Inside-R’ Framework

DTEX