EXHIBIT D

paloalto NETWORKS

Discussion of the Future and Utilization of AI and Cybersecurity Implications for Arkansas

Michael Gregg

My Background

SIGNIFICANT ACHIEVEMENTS & CONTRIBUTIONS

AUTHOR OF 2 DOZEN (24) PUBLISHED BOOKS

ASSISTED IN PASSAGE OF KEY STATE LEGISLATION

INVITED TO WHITE HOUSE TO SHARE SECURITY PROGRAM SUCCESSES

FORMER EXPAT Global C-Level Leader: Operational leadership in Asia for a massive terminal operator. Faced sophisticated international adversaries using automation for borderless, machine-speed attacks.

FORMER STATE CISO: Transformed a state security posture. **Scale: 20,000 to 250,000 endpoints.** Optimized legacy systems under tight budgets and talent shortages. **Key Insight:** State agencies must automate out of security challenges, not hire out!

PALO ALTO NETWORKS LEADER: Strategic engagement with state and local governments. Real-time visibility into global threat telemetry, analyzing billions of daily events to stop AI-driven breaches with precision security.

Introduction

Today's topics include:

- Emerging Trends and Where Is AI Today?
- The Current Threat Landscape
- Opportunities For The State of Arkansas?
- Discussion

AI Is Evolving Faster Than Anyone Predicted

1B AI app users in under two years.

"The ChatGPT launch 26 months ago was one of the craziest viral moments I'd ever seen - and we added one million users in five days. [More recently….] we added one million users in the last hour."

Sam Altman

The Future of Government: AI as a Force Multiplier

Faster Document Processing

Automates report summaries, form extraction, and document reviews to significantly reduce administrative workload.

Workforce Productivity Gains

Deploys generative AI assistants like Copilot to speed up drafting, meeting summaries, and policy search.

Benefits Fraud Detection

Leverages predictive analytics across tax and public benefit systems to detect suspicious activity at scale.

Improved Citizen Experience

Powers unified digital assistants so residents can easily access cross-agency services from a single point.

AI creates opportunity, but further complicates security

"78% who use AI at work bring their own AI tools rather than use employer provided solutions.[1]"

Shadow AI exposes the enterprise to **data leakage and malware**

Attacks on AI Apps, Models, and Data

By the end of 2026, a majority of SLED organizations are expected to have moved beyond AI pilots toward operational AI use, driven by improvements in AI governance, orchestration, and enabling platforms."

Risk from malicious inputs, LLM compromise, model-generated threats, an **data exposure**

Source 1: Microsoft's 2024 Work Trend Index https://www.secondtalent.com/resources/shadow-ai-statistics

Current Threat Landscape

New Controls For New Risks

1. AI Risks Differ From Traditional App Risks

Traditional AppSec focuses on deterministic code execution, standard inputs, and rigid SQL/API perimeters. AI applications rely on non-deterministic models, semantic reasoning, and opaque weights.

Traditional process must adapt to this new paradigm.

2. Attacks Often Mimic Normal Usage

Prompt injections, semantic data extraction, and model poisoning do not trigger conventional payload signatures. Adversaries communicate with models using natural language—the exact same interface as trusted users.

Malicious intent remains completely invisible to standard perimeter filters.

Trends Shaping The Threat Landscape in 2026

1

AI has become a force multiplier for threat actors

2

Identity has become the most reliable path to attacker success

3

Software supply chain risk has expanded beyond vulnerable code to the misuse of trusted connectivity

4

Nation-state actors are adapting stealth and and targeting state infrastructure

TREND 01

AI Is Now A Force Multiplier

AI is no longer just a concept; it is an attack accelerator

- **Vulnerability Chaining:** Frontier cyber models demonstrate a massive surge in capability to chain multi-stage exploits.
- **Strategic Access:** Early model integration via Anthropic Project Glasswing & OpenAI Daybreak Partner Program.
- **Multi-Model Discovery:** Mythos and OpenAI 5.5-cyber discover unique exploits requiring combined defense stacks.

WHY THIS MATTERS

Increased attack speed, scale, and execution consistency

Drastically lowered skill barriers for complex cyber operations

Enhanced execution efficacy fundamentally altering threat intent

Coding Leaps Translate Directly to Vulnerability Discovery

2+ Years — Equivalent pentesting capability achieved in **3 weeks** of Mythos-based scanning.

75 CVEs — Vulnerabilities covered in May Patch Wednesday vs typical baseline of **< 5 CVEs/month**.

72% — Exploits successfully created by AI models, **enabling autonomous attacks** in the future.

3–5 Mo — Expected timeframe before cyber model capabilities reach **open-source & attacker hands**.

1 SWE-bench Pro evaluates autonomous engineering on complex real-world codebases. 2,3,4 Internal testing at PANW.

Source: Anthropic Frontier Red Team Blog | Project Glasswing | PANW Analysis

TREND 02

Identity

Identity has become the most reliable path to attacker success.

Identity weaknesses played a key role in

89%

of all security investigations handled.

WHY THIS MATTERS

- **Credentials** were used to move laterally and escalate privileges
- **Identity abuse** enabled attackers to blend into normal activity
- **Identity failures** amplified downstream impact across environments

Source: Unit 42 Incident Response Data

TREND 02

Identity

OVERVIEW

- AI easily automates highly convincing, targeted social engineering via deepfakes and real-time identity mimicking.
- Hyperpersonalized phishing. Social Engineering at machine speed
- Synthetic media generated to target public officials, agency announcements, or emergency management communications.

EXAMPLE

Real-time Video Synthesis

Impact

- Attackers use real-time cloned voice calls to trick finance officers into authorizing emergency wire transfers or changing vendor direct deposit accounts.
- Increased probability state employees fall victim to a fake video message from "their IT director" asking them to re-authenticate their login credentials.
- This can undermine constituent confidence, spreads public panic during emergencies, and complicates state agency crisis management.

TREND 03

Supply Chain

Software supply chain risk has expanded beyond vulnerable code to the misuse of trusted connectivity.

+3.8X increase in attacks involving third-party SaaS applications

Rising to **23% of attacks in 2026**

22% of cases, vulnerabilities maintain a consistent level in initial access of attacks

TREND 03

Software Supply Chain Risk

Rise of Inside-Out Supply Chain Attacks

Rapid AI deployment expands an already vulnerable software supply chain, enabling attackers to **bypass perimeter defenses** and breach enterprise cores.

Recent exploits: **Salesloft, Gainsight, LiteLLM & Trivy**

Open-Source Dependencies

80% of application code is pre-built, introducing hidden vulnerabilities through third-party libraries.

AI & Model Integrity

Model poisoning risks and hidden backdoors embedded in pre-trained open-source algorithms.

Vendor Network Access

Compromised contractor credentials leveraging elevated permissions across enterprise and state systems.

Source: Unit 42 Threat Research

TREND 04

Nation State Actors

Nation-state actors are adapting stealth and persistence tactics to attack modern enterprise operating environments.

CAMPAIGN ATTRIBUTION

Across campaigns affiliated with:

- China
- North Korea
- Iran

⚠ Sophisticated actors shifting focus toward identity, cloud, and edge infrastructure.

EVOLVING STEALTH & PERSISTENCE TACTICS

1. **Identity-Driven Access**
   Greater reliance on stolen credentials and valid session tokens to blend into authorized traffic.
2. **Infrastructure & Virtualization Compromise**
   Deeper compromise targeting core hypervisors, edge devices, and virtualization layers.
3. **AI-Enabled Tradecraft**
   Early experimentation with AI tools aimed at accelerating stealth execution and long-term persistence.

Source: Unit 42 Threat Research

TREND 04

Cyber Attacks on U.S. Water Infrastructure

State-sponsored campaign targeting internet-facing operational technology and programmable logic controllers.

IMPACT SCOPE
Multiple States

ATTRIBUTION
Iran-Linked

KEY THREAT FINDINGS

Coordinated Campaign
Widespread intrusions targeting municipal water and wastewater facilities.

OT & PLC Exploitation
Targets internet-exposed Unitronics PLCs and unmanaged default credentials.

State-Sponsored Actors
CISA, FBI, and NSA attribute active disruptions to Iranian-affiliated threat groups.

Publicly Reported Activity

Minnesota	Multiple Reported
Michigan	Multiple Reported
Georgia, NJ, SD	Activity Confirmed
Additional States	Multiple Disclosed

DEFENSIVE ROADMAP

01. EXPOSURE AUDIT
Disconnect all PLCs and OT management portals directly reachable via public IPs.

02. NETWORK SEGMENTATION
Isolate operational technology networks and mandate MFA for all remote VPN access.

03. HARDENING & PASSWORDS
Replace manufacturer default passwords immediately and block unneeded open ports.

ATTACK EXECUTION SEQUENCE & KILL CHAIN

01. SCAN	02. ACCESS	03. AUTH	04. MODIFY	05. IMPACT
Internet Scan	**Port Probe**	**Default Logins**	**Logic Alteration**	**Disruption**
Probes exposed water controllers	Find exposed accessible ports	Bypasses unchanged passwords	Changes IP settings & PLC code	Causes pressure loss & manual ops

TREND 04

Cyber Attacks on U.S. Infrastructure

Nation-state and criminal actors target critical infrastructure nationwide, seeking espionage, disruption, and financial gain

IMPACT SCOPE
National Exposure

TARGETING SCOPE
Nationwide

KEY POINTS

Coordinated Campaign
Escalated attacks by nation-state actors and cybercriminals across U.S. transit agencies.

IT & OT System Targeting
Exploits focus on traffic signals, cameras, sensors, and central control networks.

Multiple Actor Motives
China, Russia, Iran, and extortion groups active for espionage, disruption, and ransom.

Ransomware Surge
Ransomware and extortion campaigns continue to target critical infrastructure organizations, increasing operational and financial risk.

WHERE IT'S HAPPENING

Examples of states with publicly reported critical infrastructure cyber incidents

West Coast & Southwest	WA, CA, OR, AZ, TX
Midwest Hubs	IL, MI, OH, MN
Southeast & Northeast	FL, GA, NC, TN, NY, PA, MA, NJ

WHY IT MATTERS & TRENDS

PUBLIC SAFETY HAZARD
Traffic management and emergency response disruptions endanger lives.

ECONOMIC & SUPPLY CHAIN DISRUPTION
Port, rail, and highway delays hit commerce and municipal budgets.

KEY ATTACK TRENDS
Targeting cloud/vendors, living-off-the-land techniques, long dwell times.

ATTACK EXECUTION SEQUENCE & KILL CHAIN

01. RECON	02. ACCESS	03. PERSIST	04. COLLECT	05. IMPACT	06. EXTORT
Asset Scanning	**Phishing & VPNs**	**Lateral Movement**	**Network Mapping**	**System Disruption**	**Ransom Demand**
Scans public portals & vendors	Exploits credentials & VPNs	Escalates internal privileges	Accesses IT/OT control systems	Deploys ransomware & halts ops	Exfiltrates data & demands ransom

THREAT ACCELERATION

In the hands of attackers, frontier cyber models will dramatically accelerate attacks

01

Vulnerability & Patch Deluge

Attackers leverage frontier AI models to find vulnerabilities at unprecedented scale. Rapid patch releases create a massive, expanding attack surface.

Impact: Automated zero-day discovery outpaces traditional patch management.

02

Autonomous Attack Workflows

Advanced models like Mythos power autonomous AI-driven exploits, compressing complex breach cycles down to minutes.

Execution: Breach timelines shrink from days or weeks to minutes.

EXPLOITATION ACCELERATION

Frontier AI Collapses the Defender Patch-and-Response Timeline

Exploitation Speed

Automated exploitation collapses attack preparation time from weeks down to minutes.

Vulnerability Chaining

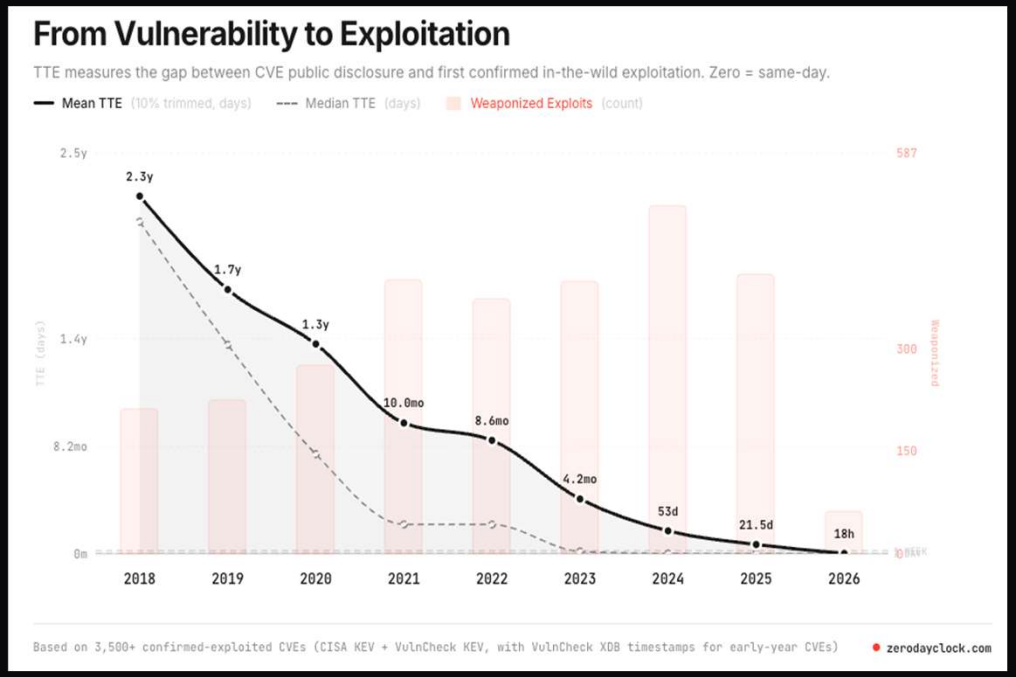
Multi-stage linkage connects minor flaws into high-impact, complex breach vectors.

Polymorphic Iterations

Machine-speed exploit mutations continuously bypass static defense signatures.

Real-Time Defense

Sub-hourly automated response replaces obsolete manual patch cycles.



Source: zerodayclock.com

Opportunities

We Must Create A Plan

We know the costs of inaction are ....

Breaches Guaranteed

50%

The percentage of organizations attacked in the last year.

Source: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026

Disruption Duration

241 Days

The prolonged business disruption and operational downtime associated with breaches lasting longer than 200 days act as the primary cost multipliers for organizations.

Source: https://www.datafence.ai/data-breach-report-2025

Financial and Business Impacts

$ 4.4 M

The global average cost of a Single Data Breach.

Source: https://www.kirkhamirontech.com/ibm-data-breach-costs-2025-report/

AI Automation Delta

$ 1.9 M

Organizations that heavily deploy security AI and automation save an average of $2 million in breach-related costs compared to those relying on manual workflows.

Source: https://www.kiteworks.com/cybersecurity-risk-management/ibm-2025-data-breach-report-ai-risks/

Consolidate To Gain Efficiency

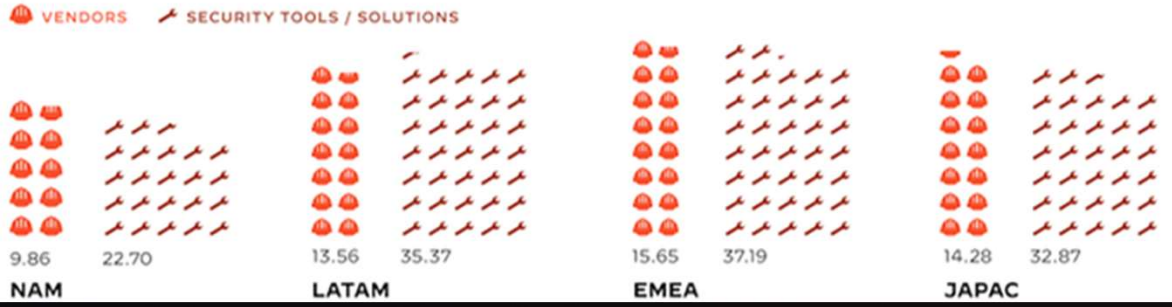
GLOBALLY

41% of organizations work with 10 or more cybersecurity vendors

NUMBER OF SECURITY VENDORS / TOOLS USED BY ORGANIZATIONS TODAY

13.39 VENDORS (TOTAL AVERAGE)

31.58 SECURITY TOOLS / SOLUTIONS (TOTAL AVERAGE)



Source: Palo Alto Networks

"Security maturity is achieved not by adding more tools, but by maximizing the effectiveness of fewer, better-integrated platforms."

The Results – Efficiency Gains

Phishing Mean Time to Resolution (MTTR)

Before redesign, 10 hours, after 55 minutes

Before

Phishing - Mean Time To Resolution - Last 7d

00 DAYS : 10 HOURS : 39 MIN

After

Phishing - Mean Time To Resolution - Last 7d

00 Days : 00 Hours : 55 Min

Phishing Mean Time to Ownership (MTTO)

Before redesign, 1 day, after 20 minutes

Before

Phishing - Mean Time to Ownership - Last 7d

01 DAYS : 00 HOURS : 55 MIN

After

Phishing - Mean Time to Ownership - Last 7d

00 Days : 00 Hours : 20 Min

Phishing Time Spent in Pre-IR

Before redesign, 1 hours, after 4 minutes

Before

Phishing - Mean Time Spent in Pre-IR - Last 7d

00 DAYS : 01 HOURS : 49 MIN

After

Phishing - Mean Time Spent in Pre-IR - Last 7d

00 Days : 00 Hours : 04 Min

STATE IMPACT & ACT 848

How Arkansas Benefits From Proper AI Implementation

OBJECTIVE Align with Arkansas legislative mandates (**Act 848 / HB 1958**) to deliver secure, compliant, and high-efficiency state services.

Client Services

- **Automation:** Intelligent processing for permits, licensing, and public benefit claims.
- **Human-in-the-Loop:** Human analysts validate and execute final policy actions.

90% Automation: AI handles initial data aggregation, correlation, and risk scoring.

Government Efficiency

- **Citizen Portals:** Replaces rigid IVR systems with intelligent agents for claims, permits, and licensing.
- **Legacy Modernization:** GenAI audits and converts decades-old mainframe code into modern secure languages.

Cost Reduction: Accelerates mainframe transformation while lowering migration overhead.

Consolidated Platform

- **Eliminate Point Add-Ons:** Avoid disconnected AI tools that inflate complexity and security blind spots.
- **Unified Cyber Defense:** Deploys AI over a clean, centralized data layer (Cortex XSIAM & Prisma).

Unified Layer: Protects both network operations and state-wide cyber infrastructure.

Source: Arkansas General Assembly (Act 848 / HB 1958)

COMMITTEE DISCUSSION

"AI is an accelerator, it will either accelerate state efficiency and defense, or it will accelerate adversary intrusion. Governance, visibility, and machine-speed defense determine which side of that line state government lands on."

Thank you for your leadership in safeguarding Arkansas!

Questions & Discussion