
go
cyber
COLLECTIVE

August Announcements

Serving Our Communities

- Thank You, Keeper Security!
- Municipal Cyber Summit
- Cyber 101 of Law Enforcement: Sept. 9
- Workshops coming: HIPPA Sept. 2, LEADS Nov. 4
- AXIS Experience Vehicle Sept. 10

August GoCyber Collective Keynote Speaker

- Ken Smith
- Director, Sales Engineer – Arctic Wolf
- "..in depth knowledge and great strategic plans"… "most valued mentors I have"… "always has time to explain a concept"
- Current state of physical pentesting

PENTESTING

ARE YOU ASSUMING YOU'RE SAFE?

WHOAMI

- **Ken Smith**, Arctic Wolf
- Director of Enterprise Sales Engineering
- **Formerly**
  - Director of L&D, *Praetorian*
  - National Lead, Cyber Testing, *RSM US*
  - Red Team, *Bank of America*
  - SIGINT Operator, *5th Special Forces Group (Airborne)*
- **Academia**
  - Former Professor of Network Security, *University of Mount Union*
  - Former Research Proposal Coordinator, *SANS Tech Institute*
- **Education**
  - MA, Security Policy Studies, *Notre Dame College*
  - AA, Arabic, *Defense Language Institute*
  - BS, Computer Info Systems, *University of Dayton*
  - OSCP, OSWP

AGENDA

- Introduction
- Evolution of Cyber Threats
- Effective Modern Offensive Security
- Ongoing Assessments
- Vulnerability Management
- Operationalizing the Findings
- Wrap-up

INTRODUCTION

- Cyber security is hard…
- Modern threat landscape includes all kinds of sophisticated threat actors and attack chains
- A lot of misconceptions and misrepresentations
- Key objectives of the presentation
  - Perspective of an offensive security professional
  - Sort out the buzzwords of modern offerings
  - *What really matters* when it comes to offensive security?

INTRODUCTION – *WHY THIS MATTERS…*

- Cyber threats have expanded to new spaces
  - GitHub + self-hosted runners
  - LLM applications (see MITRE's ATLUS)
- Attackers *still* prioritize well-known paths
- Tackle the new without forgetting the old

THE EVOLUTION OF CYBER THREATS

EVOLUTION OF CYBER THREATS – *10 YEARS AGO…*

- 2012 – 2015 was a golden age for testers
  - Phishing with Excel macros
  - Encoded PowerShell payloads
  - Mimikatz as a Metasploit plugin (‘fileless malware’)
- All of these things are very likely to get caught today
  - But the broader vectors are still relevant
  - Phishing is as big as ever, credentials are still king

EVOLUTION OF CYBER THREATS – *DEFENSES FALL SHORT*

- Traditional defenses like firewalls and antivirus tools
  - No longer sufficient *(that doesn't mean get rid of them…)*
  - Attack surfaces have gotten too big
  - Why attack the org directly?
    - Supply chain attacks
    - Cloud environments
- Need to approach security operationally – *Test your stuff!*

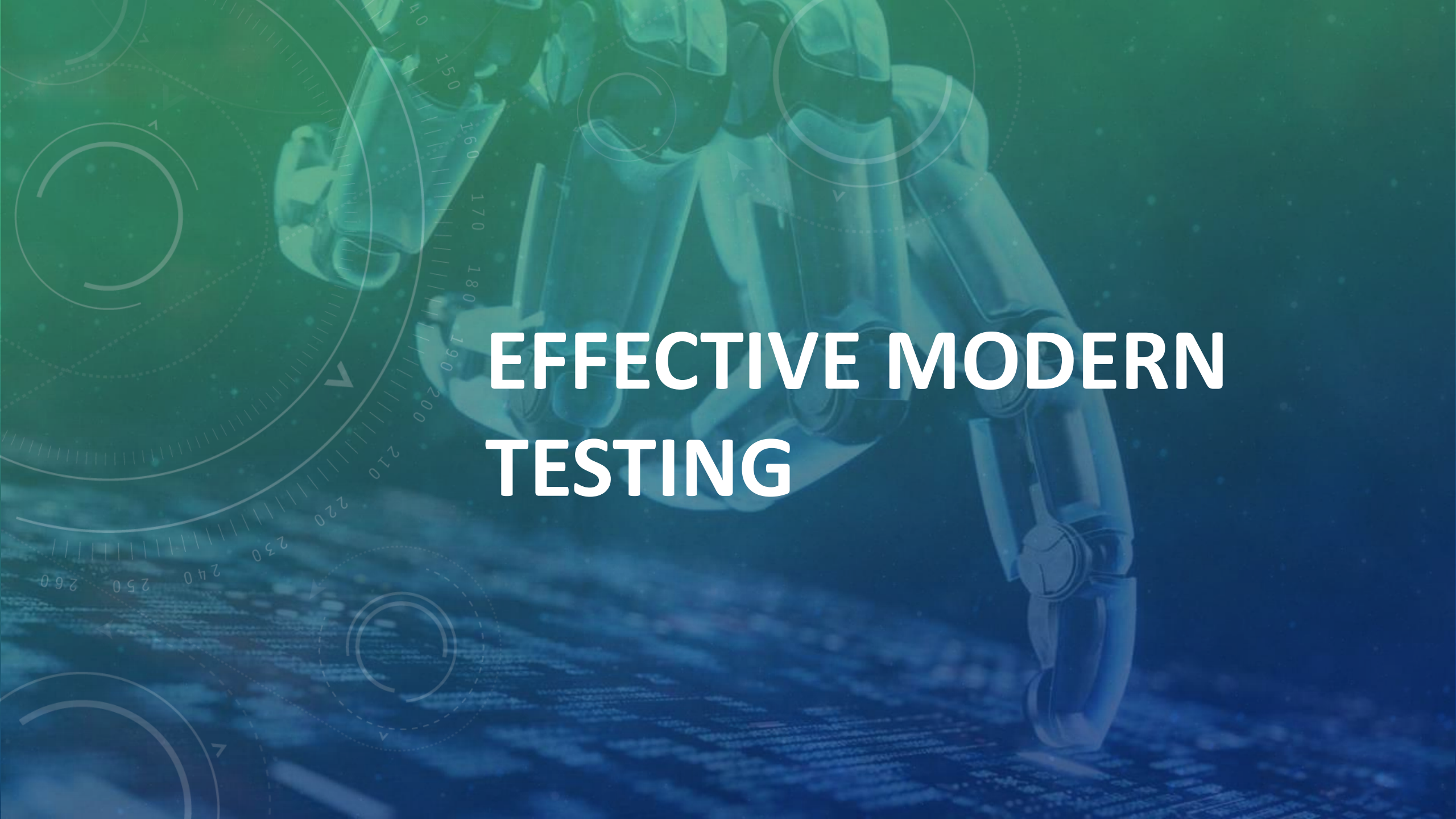
EVOLUTION OF CYBER THREATS – *EMERGING ISSUES*

- Remote work setup
  - Same old vector…
  - Poorly secured VPN (~flat networks)
  - Insufficient training – Fake VPN login portals
- Device code phishing in cloud services
  - Attackers target cloud services
  - Users authenticate to malicious apps/sites
  - Bypasses traditional defense mechanisms

EVOLUTION OF CYBER THREATS – *OLD IS NEW…*

- The techniques change, but the vectors stay the same
  - 80% of cloud breaches are related to credentials
  - We're still collectively reusing passwords
  - Pass-the-Hash is still viable for lateral movement in 2025
  - Vishing is back with a vengeance

- Don't get distracted!



EFFECTIVE MODERN TESTING

MODERN TESTING – *SCOPING*

- Modern pentesting requires careful scoping
  - Asset identification and classification
  - Even as granular as app components
  - Get the testing team involved!

- You can’t have a good test without knowing your network
  - Be involved in the scoping process
  - Testers can’t/shouldn’t be touching anything without written permission

EFFECTIVE MODERN TESTING – *THREAT MODELING*

- Under utilized tool in the industry
- Reinforces your asset classification – *really, this* is *classification*
- Threat modeling minimizes the chance of unturned stones
- Work it internally first, and get tester input
  - You know your company
  - Nightmare scenarios?
  - PASTA - **P***rocess for* **A***ttack* **S***imulation and* **T***hreat* **A***nalysis*

PASTA Threat Modeling Stages

The output of each stage provides input for the next stage

Stage One Define the Objectives

Stage Two Define the Technical Scope

Stage Three Decompose the Application

Stage Four Analyze the Threats

Stage Five Vulnerability Analysis

Stage Six Attack Analysis

Stage Seven Risk and Impact Analysis

EFFECTIVE MODERN TESTING – *CATEGORIES*

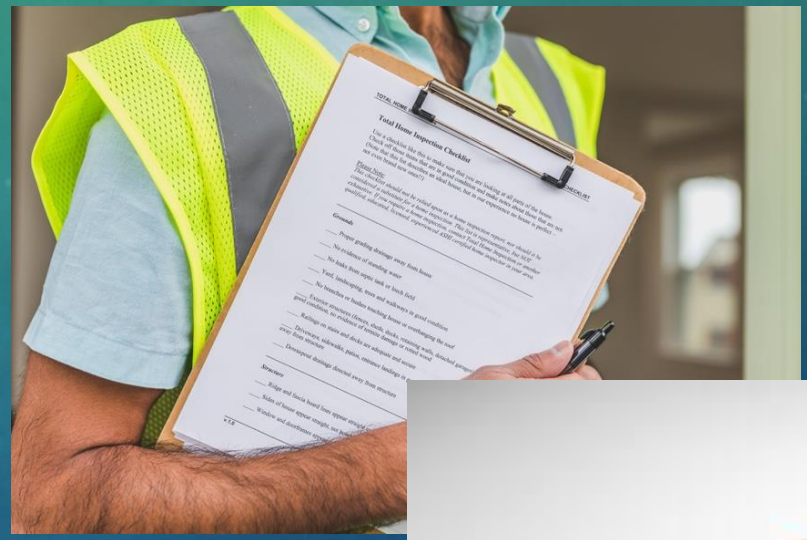
- Vulnerability Scanning
- Penetration Testing
  - Network
  - Application
  - Device/hardware
- Red Teaming
- Purple Teaming
- Continuous testing

EFFECTIVE MODERN TESTING – *CATEGORIES*

- ***Vulnerability Scanning***
- Penetration Testing
  - Network
  - Application
  - Device/hardware
- Red Teaming
- Purple Teaming
- Continuous testing

EFFECTIVE MODERN TESTING – *CATEGORIES*

- Vulnerability Scanning
- ***Penetration Testing***
  - Network
  - Application
  - Device/hardware
- Red Teaming
- Purple Teaming
- Continuous testing



EFFECTIVE MODERN TESTING – *CATEGORIES*

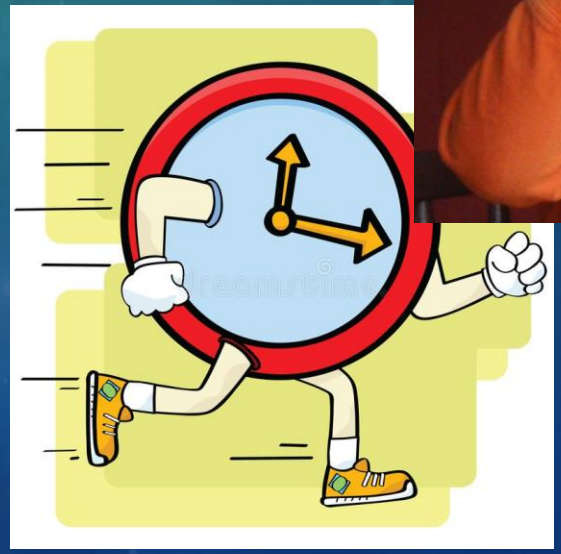
- Vulnerability Scanning
- Penetration Testing
  - Network
  - Application
  - Device/hardware
- ***Red Teaming***
- Purple Teaming
- Continuous testing

EFFECTIVE MODERN TESTING – *CATEGORIES*

- Vulnerability Scanning
- Penetration Testing
  - Network
  - Application
  - Device/hardware
- Red Teaming
- ***Purple Teaming***
- Continuous testing

EFFECTIVE MODERN TESTING – *CATEGORIES*

- Vulnerability Scanning
- Penetration Testing
  - Network
  - Application
  - Device/hardware
- Red Teaming
- Purple Teaming
- ***Continuous testing***




ONGOING
ASSESSMENT

ONGOING ASSESSMENT

- Annual testing and quarterly scanning have their places
- Point-in-time assessments
- Continuous testing is an attractive prospect – But challenging
  - Too much automation means mountains of false positives
  - Too many people means slow, expensive testing
- Security operations is probably where this ultimately ends up

ONGOING ASSESSMENT

- Continuous testing breaks the traditional model
  - Scanning is about finding vulnerabilities
  - Pentesting is about linking vulnerabilities
  - Red Teaming/Purple Teaming are about response/readiness
  - Continuous testing is…antivirus for vulnerabilities?

- We're all still figuring this out…

ONGOING ASSESSMENT – *ACRONYM SALAD*

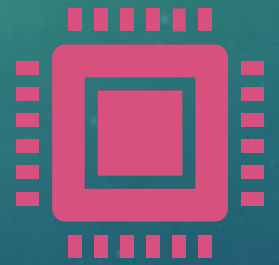
- **CPT**: *Continuous Penetration Testing*
- **PTaaS**: *Penetration Testing as a Service*
- **CTEM**: *Continuous Threat Exposure Management*
- **ASM**: *Attack Surface Management*
- **EASM**: *External Attack Surface Management*
- **CASM**: *Continuous Attack Surface Management*

ONGOING ASSESSMENT – *QUESTIONS*

Compliance

Governance, Risk, and Compliance?

Lingering Regulatory Questions



Methods and Depth of testing

Vendor and solution dependent

You may not end up with Attack Paths

Vuln scanning with extra steps?

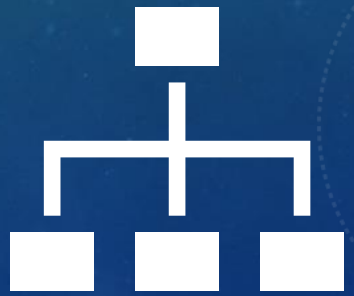
Outsourced testing teams

VULNERABILITY MANAGEMENT

VULNERABILITY MANAGEMENT

- Once a penetration test is completed, the real work begins:
  - Triaging findings
  - Assigning severity
  - Establishing remediation plans

- Just like asset management is important up front…
  - Vulnerability management is important at the end
  - You need a plan and system for all of this



VULNERABILITY MANAGEMENT

- Consider aligning to a framework(s)…
  - Cyber Kill Chain
  - MITRE ATT&CK
  - MITRE ATLAS
  - CIS Critical Security Controls
  - OWASP Top Ten


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (4)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (8)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (7)
- Stage Capabilities (6)

Initial Access
11 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)
- Wi-Fi Networks

Execution
16 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (12)
- Container Administration Command
- Deploy Container
- ESXi Administration Command
- Exploitation for Client Execution
- Input Injection
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution

Persistence
23 techniques

- Account Manipulation (7)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Cloud Application Integration
- Compromise Host Software Binary
- Create Account (3)
- Create or Modify System Process (5)
- Event Triggered Execution (17)
- Exclusive Control

Privilege Escalation
14 techniques

- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- Account Manipulation (7)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (5)
- Domain or Tenant Policy Modification (2)
- Escape to Host
- Event Triggered Execution (17)
- Exploitation for Privilege

Defense Evasion
45 techniques

- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (2)
- Email Spoofing
- Execution Guardrails (2)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)

Credential Access
17 techniques

- Adversary-in-the-Middle (4)
- Brute Force (4)
- Credentials from Password Stores (6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (9)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request

Discovery
33 techniques

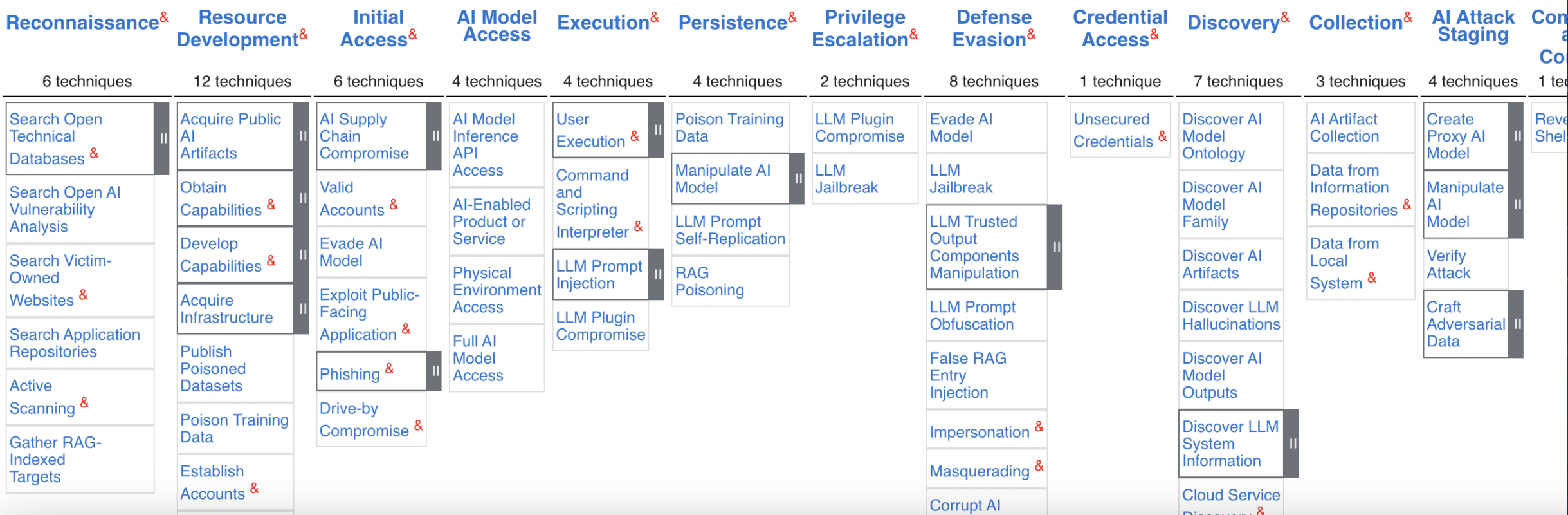
- Account Discovery (4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

ATLAS Matrix

The ATLAS Matrix below shows the progression of tactics used in attacks as columns from left to right, with ML techniques belonging to each tactic below. & indicates an adaption fron
Click on the blue links to learn more about each item, or search and view ATLAS tactics and techniques using the links at the top navigation bar. View the ATLAS matrix highlighted alo
ATT&CK Enterprise techniques on the ATLAS Navigator.



CIS Critical Security Controls Navigator

Want to see how the CIS Critical Security Controls fit into your broader security program? Use our CIS Controls Navigator to explore how they map to other security standards.

CIS Controls v8.1

Follow these steps to get started with the CIS Controls Navigator

STEP 1

Select your version of the CIS Controls

Select which version of the Controls you are currently usin
earlier versions no longer supported on the Controls Navig
select the option to access WorkBench.

1 2 3 4 5 6

Currently vie

Mappings

IG1 IG2 IG3

HIDE UNSELECTED SAFE

VULNERABILITY MANAGEMENT

- The report and read-out are the most important parts of a test

- Collaborative report and remediation process
  - Reports should capture mitigating factors/positives
  - Edits should never get political no matter how painful
  - Remember that there will always be something found
- Be sure to look for tactical and strategic recommendations

VULNERABILITY MANAGEMENT – *RISK*

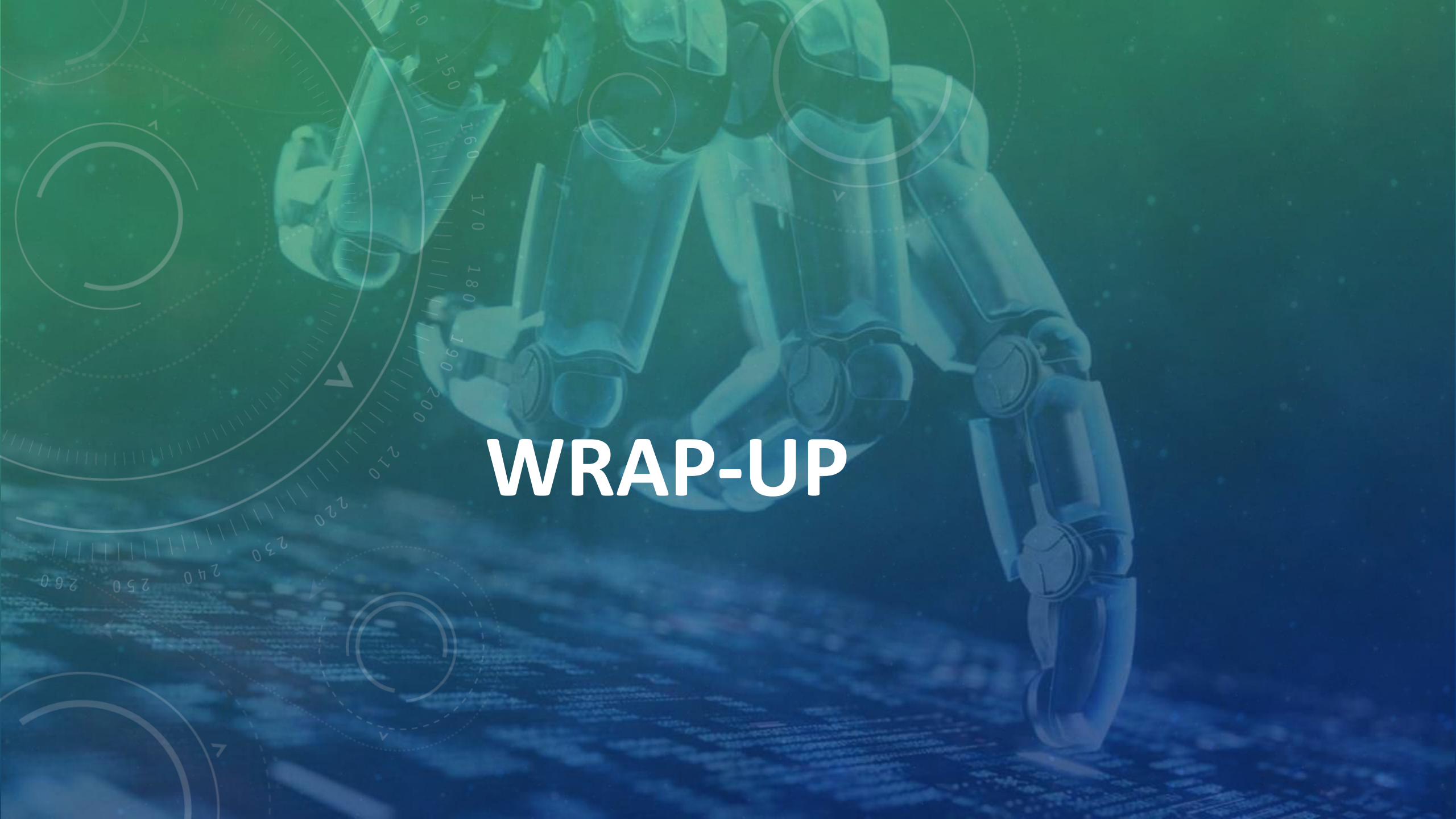
- How do we translate to risk then?
  - Near infinite number of methods and platforms available
  - Find something that works for your organization
  - You need to be able to capture more than the pentest
    - MS17-10 on your domain controller
    - MS17-10 on a DMZ web server, off-domain
- Almost certainly a full-time role…

VULNERABILITY MANAGEMENT – *SCORING*

- It's very important to be able to quickly rack and stack findings
- A *lot* of firms develop proprietary methods to emulate risk
  - Weight averages
  - Unique formulas
- Offensive security testing will never yield a risk score *ever*
  - Risk is [Threat * ***Vulnerability*** – *Controls]*
  - Don't fall for it, and don't ask for it
  - Stick to CVSS (2.0 if you can…)

VULNERABILITY MANAGEMENT

- Prioritize vulnerabilities based on the established scoring
  - Business impact
  - Likelihood of exploitation
  - Environmental factors
- Look for common root causes
  - Passwords / account management
  - Patch management



WRAP-UP

WRAP-UP

- Techniques change, but the big picture rarely does
- Penetration testing is an ongoing process, not a one-off task
  - Continuous testing is coming…eventually
  - Effective vulnerability management is critical
- Plan your testing
  - Scanning? App testing? Something more advanced?
  - Work it into your risk plan
  - Don’t forget to threat model!


Q&A

August GoCyber Collective Spotlight

- David Sutherin
- Founder & Cyber Compliance Program Director – Triumvirate Cybersecurity Consulting
- CMMC for the Little Guy: January 27

CYBER COMPLIANCE

CRASH COURSE FOR FEDERAL & DEFENSE CONTRACTORS

Triumvirate Cybersecurity | August 2025

tri • um • ver • et

www.triumviratecyber.

About Triumvirate Cybersecurity

- **We Provide Accredited Cyber Compliance Services**
  - We primarily serve members of the Defense Industrial Base in preparation for CMMC as a **CyberAB Registered Practitioner Organization (RPO)**
  - Our services include gap assessment, policy & procedure development, project management, ongoing compliance maintenance, and more
  - Our newest offering—**CMMC Enclave as a Service**—is designed to be an "easy button" for companies through managed IT and compliance services
- **We Focus on Small & Midsize Businesses (SMBs)**
  - Small businesses often lack compliance expertise needed to comply
  - SMBs are underserved by larger consulting firms

Cybersecurity in Federal Contracting

- Executive Order 13556 (2010): Instructed Federal agencies to standardize protection of **Controlled Unclassified Information (CUI)**
  - **CUI**: Government information protected by law, regulation, or government-wide policy & listed in the NARA CUI Registry
- FAR 52.204-21 (2016): 15 “basic safeguarding” requirements for contractor systems housing any **Federal Contract Information (FCI)**
  - **FCI**: Information not intended for public release provided by or generated for the government under a contract

Executive Order 13556 -- Controlled Unclassified Information

FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

Examples of Controlled Information

Federal Contract Information (FCI)
A signed government contract
A purchase order on a supplier portal
Emails to/from a Contracting Officer (CO)
Contract performance data
Project plans referencing gov requirements
Information about subcontractors

Is the information meant for public disclosure?

Controlled Unclassified Information (CUI)
Defense controlled technical information (CTI)
Critical infrastructure emergency mgmt. info
Export controlled products/research
Law enforcement communications
Student records under FERPA
Patient health records

Is the information governed by law/regulation?

Intro to the CMMC Program

- The DoD's **Cybersecurity Maturity Model Certification**
- Created to address issues with contractor self-attestation of compliance with **NIST SP 800-171** (Rev 2) for CUI handling
- Includes 3 certification levels with varying requirements depending on level of access to sensitive information
- Higher levels require audit by a **Third-Party Assessor Organization (C3PAO)**

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CMMC Levels

Level 1

- Applies to all DoD suppliers
- **15 requirements** (FAR 52.204-21) assessed via annual self-attestation

Level 2

- Applies to suppliers with access to CUI
- **110 requirements** (NIST SP 800-171) assessed by a C3PAO
- Annual self-assessment + triennial re-certification

Level 3

- Applies to suppliers w/ access to certain sensitive types of CUI (e.g., nuclear)
- Level 2 assessed by C3PAO
- **35 additional requirements** (NIST SP 800-172) assessed by DIBCAC
- Annual self-assessment + triennial re-certification

CMMC Timeline

- **CMMC is starting to show up in contracts** as a provisional r
- Office of Management & Budget (OMB) **final review bega**
- Rollout expected to begin **by the end of 2025**

Contracting Officers (COs) are **already considering CMMC readiness** when evaluating bids

2010
E.O. 13556

2016
FAR 52.204-21

2017
DFARS 252.204-7012

2020
DFARS 252.204 -7019, -7020, -7021 & CMMC v1.0 Proposed

2023
CMMC v2.0 Proposed

2024
32 CFR 170 formally establishes CMMC program

YOU ARE HERE

2025
Finalization of 48 CFR 252.204-201 &
CMMC rollout Phase 1 **mandates CMMC for DoD suppliers**

2026
CMMC rollout Phase 2

2027
CMMC rollout Phase 3

2028
CMMC fully implemented

The FAR CUI Rule

- **Will apply CMMC-like requirements to** all federal contractors
  - This was the intent of Executive Order 13556—DoD just first
  - Also mandates documented compliance with **NIST SP 800-171**
- 👎👎 **Public draft released in January 2025 (FAR Case 2017-016)**
  - **Does not** include a phased rollout
  - 👍 Defines **contractor liability** in the event of data breaches impacting CUI and **reduces reporting timeline to 8 hours** (down from 72 hours)
  - 👍 Unlike CMMC, draft rule **does not** require third-party certification

How to Prepare for Compliance

- Determine if You Handle FCI/CUI: Review contracts, project scopes, and communications with federal agencies. Contact COs, if necessary
- Decide on Scope: Determine whether your entire organization needs access to controlled information or if a secured enclave is more appropriate
- Conduct a Gap Assessment: Compare your existing security measures against NIST SP 800-171
- Develop a System Security Plan (SSP): This document outlines your organization’s cybersecurity program & security measures
- Implement Necessary Controls: Begin addressing identified gaps by

TRIUMVIRATE
CYBERSECURITY

Thank You

For more information, please visit our website, check out our blog, sign up for our newsletter, or contact us at info@triumviratecyber.org to schedule a free consultation

August GoCyber Collective Spotlight

- Nate Henderson
- AXIS Communications
- GoCyber Collective Field Trip to the Parking Lot
- AXIS Experience Vehicle – Sept. 10

Innovating for a

smarter, safer world.

Axis at a Glance

1984 — **Axis is founded** by Keith Bloodworth, Martin Gren and Mikael Karlsson

1996 — **Inventing network video** with AXIS 200 Network Camera

1999 — Developing the industry's first System-on-Chip specifically for video surveillance: **ARTPEC**

2004 — Launching our first **partner program** for channel partners

2005 — Establishing the **Axis Communications Academy**

2007 — Signing the **UN Global Compact** agreement

2013 — Entering the **physical access control** market by launching our first door controller

2015 — Developing Axis **Zipstream** technology

2020 — Entering the **body worn camera** market with our first body worn camera

2024 — Releasing **Axis Cloud Connect** an open hybrid cloud platform, enabling managed services

Releasing the 9th version of **ARTPEC**, with support for the proven AV1 encoding standard

Products & Solutions

Network cameras

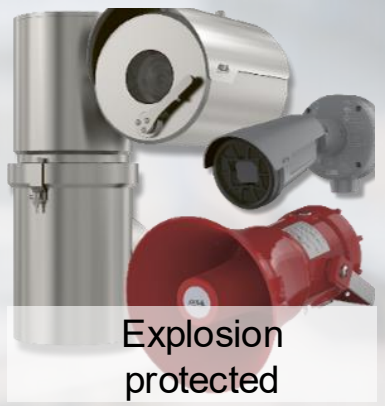
Analytics

Access control

Network intercoms

Network audio

Wearables



Explosion protected

Management software

Video recorders & workstations

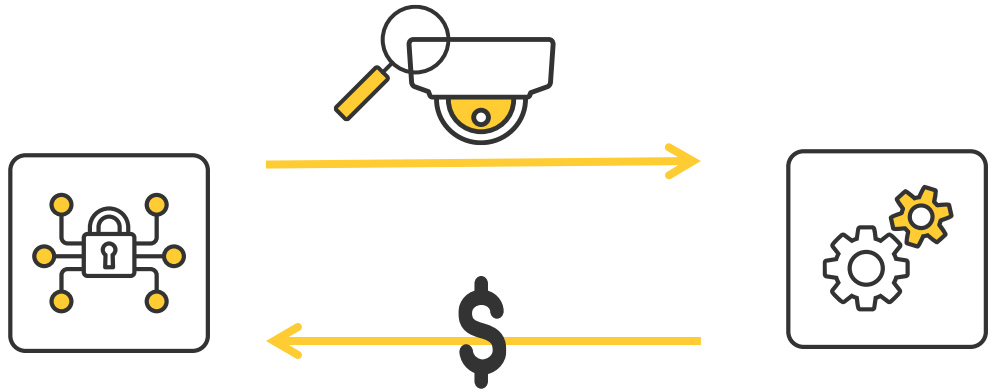
System devices

Accessories


AXIS
COMMUNICATIONS
Axis Approach
to Cybersecurity

Cybersecurity Considerations

- > Software Bill of Materials
- > Bug Bounty Program
- > FIPS 140 Certified
- > CVE Numbering Authority
- > Zero Trust Networking
- > Security Patches Provided for an Average of 10 Years



THE Axis Experience **Vehicle**

2025 Mid-Atlantic Tour

Experience Innovation on Wheels with the Axis Experience Vehicle

The Axis Experience Vehicle (AEV) brings the future of security and surveillance directly to you.

Designed as a mobile extension of our Axis Experience Center, this 39-foot, state-of-the-art vehicle delivers hands-on access to the latest innovations in security, analytics, and network solutions—all in real-time, right in your area.

Discover Countless Axis Solutions

- > Air Quality Sensor
- > Network Display Speakers
- > Audio Analytics
- > AXIS Camera Station Pro
- > ARTPEC-9 SoC with AV1 support
- > Smart Search 2 with free text search

Save the Date!

When: Wednesday, Sept. 10th, 10am - 4pm

Where: 201 Tyler Way, Moraine, OH 45439

Come and go as you please,
lunch will be provided!

Get your free tickets **now!**

2N BriefCam Genetec milestone RUCKUS COMMSCOPE sound intelligence

THANK YOU

Get your free tickets **now!**

● CONNECT

August GoCyber Collective Spotlight

- Nancy Percy
- Business Dev. Manager - Workforce Development
- Sinclair College
- GoCyber Collective Leadership Conference

Sinclair Workforce Development Leadership Series

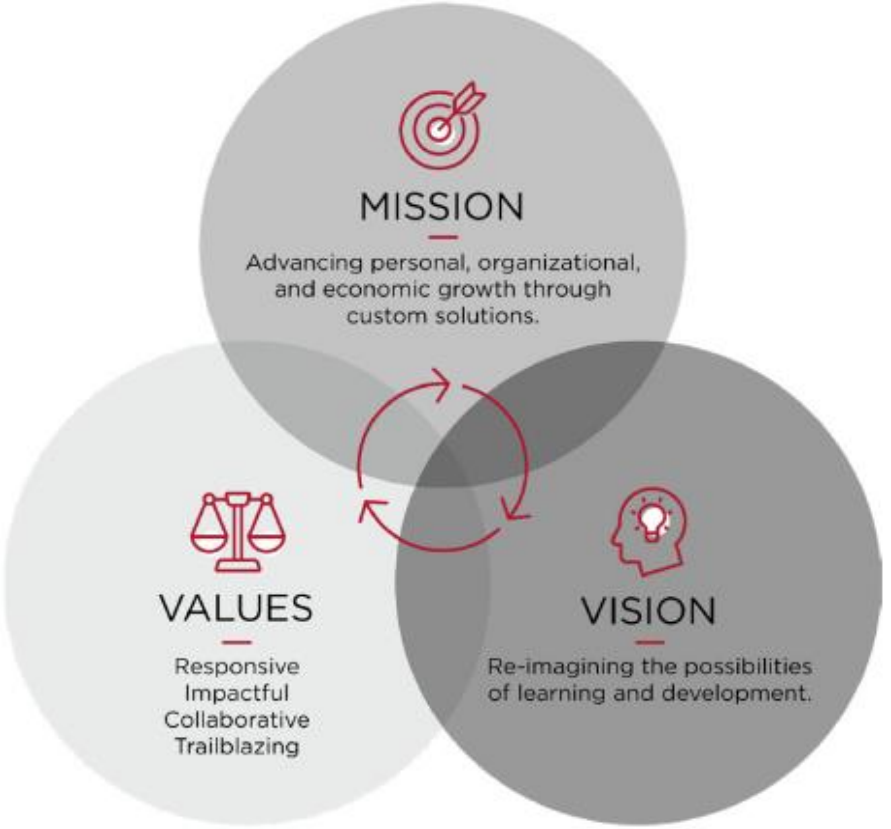
SINCLAIR
Workforce Development

ABOUT US

We strive to support founder David Sinclair's mission to

"Find the need and endeavor to meet it."

By partnering with local industry leaders, Sinclair Workforce Development provides consulting, training, certifications, custom training **solutions, and resources relevant to the demands of today's job market**.



SINCLAIR
Workforce Development

PRACTICE AREAS

INDUSTRY CERTIFICATIONS

LEADERSHIP AND ORGANIZATIONAL EFFECTIVENESS

SAFETY TRAINING

Goldman Sachs 10,000 small businesses

OPEN ENROLLMENT AND ELEARNING

MANUFACTURING SKILLS TRAINING

SKILLS-BASED ASSESSMENTS

Ohio | TechCred

SINCLAIR
Workforce Development

Workforce Development Series

Foundational Leadership Series	Emerging Leaders
Supervisor Series	Supervisors

SINCLAIR
Workforce Development

Why invest in training?

SINCLAIR
Workforce Development

Source: "Leadership Transition Report 2021," Development Dimensions International, Inc.,2021

Foundational Leadership Series

Unleashing Your Leadership Potential

Communication that Connects

Managing Conflict with Confidence

SINCLAIR
Workforce Development

Foundational Leadership Series

Building a Culture of Accountability

Feedback: The Art of Giving and Receiving

The Inclusive Leader

SINCLAIR
Workforce Development

Supervisor Series

Developing Your Team: Strategies for Supervisors

Taking Back Your Time

Strong Teams Start with Trust

SINCLAIR
Workforce Development

Supervisor Series

Coaching for Performance and Growth

The Engagement Factor

Navigating the Waters of Change

SINCLAIR
Workforce Development

Sinclair in Centerville

Sinclair in Mason

Or let us come to YOU!

SINCLAIR
Workforce Development

Have a Remote Team?

We are Hybrid-Ready

SINCLAIR
Workforce Development

Our Participants Make the Difference

Questions?

Nancy Percy
Business Development Manager
nancy.percy@sinclair.edu
937-672-7049

SINCLAIR
Workforce Development

August GoCyber Collective Sponsor

- Nate Albert
- Channel Account Manager
- Keeper Security
- GoCyber Collective Leadership Conference

KEEPER + FedRAMP

Why Legacy PAM Is a Risk You Can't Afford

Discover the Keeper Advantage

Today's cyber threats demand more than outdated tools — they require a modern, agile approach to security. **If your organization still relies on a legacy Privileged Access Management (PAM) solution, you're not just behind the curve — you're at risk**. Let us show you how **Keeper Security** is redefining privileged access management with an unparalleled zero-trust approach.

Outdated PAM solutions are a liability

Legacy PAM systems were designed for a world of static networks and secure perimeters. But in today's fast-paced, cloud-native world of hybrid environments and remote work, these outdated solutions leave critical vulnerabilities:

01 Gaps in security

Legacy PAM requires multiple firewall openings (ports 443, 80, 22, etc.), creating a porous network that's ripe for exploitation.

02 Underutilized complexity

Many organizations deploy only a limited number of legacy PAM features, creating shadow IT issues and a false sense of security.

03 Cloud-native disconnect

Legacy systems can't keep up with modern CI/CD pipelines, dynamic secrets management or automated secret rotation.

The result? Increased attack surfaces, inefficiency and operational bottlenecks.

Why organizations of all sizes choose Keeper

Keeper is the **zero-trust, cloud-native PAM solution** built for the challenges of today and tomorrow. Here's how Keeper solves problems that legacy PAM systems can't:

Perimeterless security with zero-trust

- No open firewall ports required.
- Every access request is authenticated and encrypted at the device level.

Seamless DevOps integration

- API-first design integrates with CI/CD workflows.
- Automated secret injection and rotation ensure secrets stay secure without slowing developers down.

Ironclad zero-knowledge encryption

- Each record is encrypted individually using **AES-256** GCM, ensuring no single breach compromises your entire system.

Simplified deployment and full utilization

- User-friendly design eliminates shadow IT and ensures every feature works out of the box.
- Teams adopt Keeper effortlessly, avoiding cumbersome workarounds.

Advanced compliance & audit capabilities

- Comprehensive logging and reporting integrate seamlessly with SIEM systems.
- Full visibility ensures compliance with evolving regulations, including GDPR, HIPAA and more.

KEEPER®

The Keeper edge: Built for the modern era

Unlike legacy solutions patched to accommodate cloud technologies, Keeper was built for the cloud from day one:

- **FedRAMP Authorized and available in the AWS GovCloud:** High availability with global data sovereignty options.
- **Double encryption:** Data at rest is encrypted locally, while data in transit uses TLS 1.3 with an additional payload encryption layer.
- **Breach prevention:** Features like **BreachWatch**® actively monitor for compromised credentials without exposing sensitive data.

Empower your security with Keeper

When you switch to Keeper, you're not just getting a PAM solution — you're future-proofing your organization. Our platform combines cutting-edge technology, zero-trust architecture and seamless integration to ensure:

- **Reduced attack surfaces** and fewer vulnerabilities.
- **Improved operational efficiency** without sacrificing security.
- **Regulatory compliance** with the most advanced encryption and logging capabilities.

Act now before it's too late

Don't let your legacy PAM solution become your Achilles' heel. Let Keeper Security empower your organization with modern, scalable and ironclad privileged access management.

Schedule a demo today to see how Keeper can revolutionize your organization's security posture while driving business agility.

About Keeper Security

Keeper Security is a leader in zero-trust and zero-knowledge cybersecurity solutions, trusted by thousands of businesses worldwide. Learn why organizations across industries choose Keeper to protect their most sensitive data.

Your security deserves more than a legacy solution. Make the move to Keeper today.

KEEPER®

KEEPER

Keeper Security

Sales Qualifying Questions for Partners

Keeper Password Manager

Enterprise Password Security & Compliance

- ✓ How does your organization currently manage employee passwords and prevent credential reuse?
- ✓ Are you struggling with enforcing password policies across teams while maintaining compliance (NIST, CMMC, FedRAMP, StateRAMP, GDPR)?
- ✓ Do you have visibility into weak, reused or compromised passwords across your organization?
- ✓ Would you like to eliminate password-related breaches and phishing risks while simplifying user access?

Keeper Secrets Manager

Secure Storage & Management of API Keys, Certificates, & Secrets

- ✓ How do your DevOps, IT and security teams store and share API keys, database credentials and certificates?
- ✓ Are secrets being stored in plaintext, spreadsheets or code repositories, posing a security risk?
- ✓ Do you need an automated, FedRAMP- and StateRAMP-authorized solution for secure secrets management?
- ✓ Would you benefit from a zero-trust, zero-knowledge approach that eliminates credential sprawl and unauthorized access?

Keeper Connection Manager

Privileged Access Management & Remote Session Security

- ✓ How do you secure remote access for privileged users and system administrators?
- ✓ Are you looking for a secure, browser-based alternative to traditional VPNs, RDP and SSH tools?
- ✓ Do you have real-time visibility into who is accessing critical systems and when?
- ✓ Would you like a FedRAMP- and StateRAMP-authorized Privileged Access Management (PAM) solution without agents or VPNs?
- ✓ How do you currently provide secure access to cloud and on-prem applications for remote teams?
- ✓ Are VPN limitations causing performance and security challenges in your organization?

KEEPER®

Keeper Remote Browser Isolation (RBI)

Secure, Isolated Web Access for End Users

- ✓ How do you protect employees from phishing, malware and browser-based threats?
- ✓ Would you like a way to prevent credential theft and session hijacking without disrupting workflows?
- ✓ Are you interested in a solution that allows users to browse the web safely, isolating all threats before they reach your network?
- ✓ Do you require a FedRAMP- and StateRAMP-authorized web security solution that neutralizes browser-based cyber risks?
- ✓ Would you benefit from only allowing employees to navigate to a pre-approved list of URLs within a secure browser environment?

KeeperPAM

Privileged Access Management

- ✓ How are you protecting access to your servers, databases and SaaS web apps?
- ✓ Do you have a clear understanding of who has access to your most sensitive systems and what exactly they are doing with it?
- ✓ What challenges do you face in regularly updating and rotating privileged credentials to reduce security risks?
- ✓ Do you have users who require Just-In-Time (JIT) or temporary access to critical systems?

About Keeper Security

Keeper Security is transforming cybersecurity for thousands of organizations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by federal agencies including the Departments of Justice and Energy to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access and remote browser isolation. Keeper is FedRAMP and StateRAMP Authorized, SOC 2 compliant, FIPS 140-3 validated, as well as ISO 27001, 27017 and 27018 certified. Learn how Keeper can defend your organization against today's cyber threats at KeeperSecurity.com.

KEEPER®

KEEPER PASSWORD MANAGER

Enterprise Password Manager

Prevent breaches, reduce help desk costs and ensure compliance.

Challenges

Weak and stolen passwords, credentials and DevOps secrets are a leading cause of data breaches. Most organizations lack visibility into these threats, with no way to enforce security best practices across every employee, in every location, across every device, application and system. This creates a series of challenges for IT admins.

01

Organizations are becoming increasingly complex and consist of human and machine credentials that need to be protected.

02

Modern ways of working with distributed remote work and multi-cloud computing have made traditional IT perimeters obsolete, increasing risk for everyone.

03

Attack surfaces are expanding exponentially as billions of additional devices, credentials and secrets are connected to distributed networks - both on and off-premises.

04

Conventional cybersecurity solutions are siloed in nature, creating critical gaps in visibility, security, control, compliance and reporting.

Organizations that don't address these core challenges face a heightened risk of data breaches, compliance violations and operational friction.

Solution

Keeper Enterprise Password Manager monitors and protects every user on every device across an organization with full cloud and native-application capabilities. Keeper seamlessly integrates with existing IT technology, including Security Information and Event Management (SIEM), Multi-Factor Authentication (MFA), passwordless and Identity Provider (IdP) solutions.

Keeper provides comprehensive authentication and encryption across every website, application and system employees interact with. The platform is easy to deploy, easy for non-technical users to adopt and is the most secure product of its kind. Keeper holds the industry's longest-standing SOC 2 Type I and II compliance and is ISO 27001, 27017 and 27018 certified as well as FedRAMP and StateRAMP Authorized.

Don't get hacked.

Learn more
keepersecurity.com

Start a free trial today
keeper.io/try

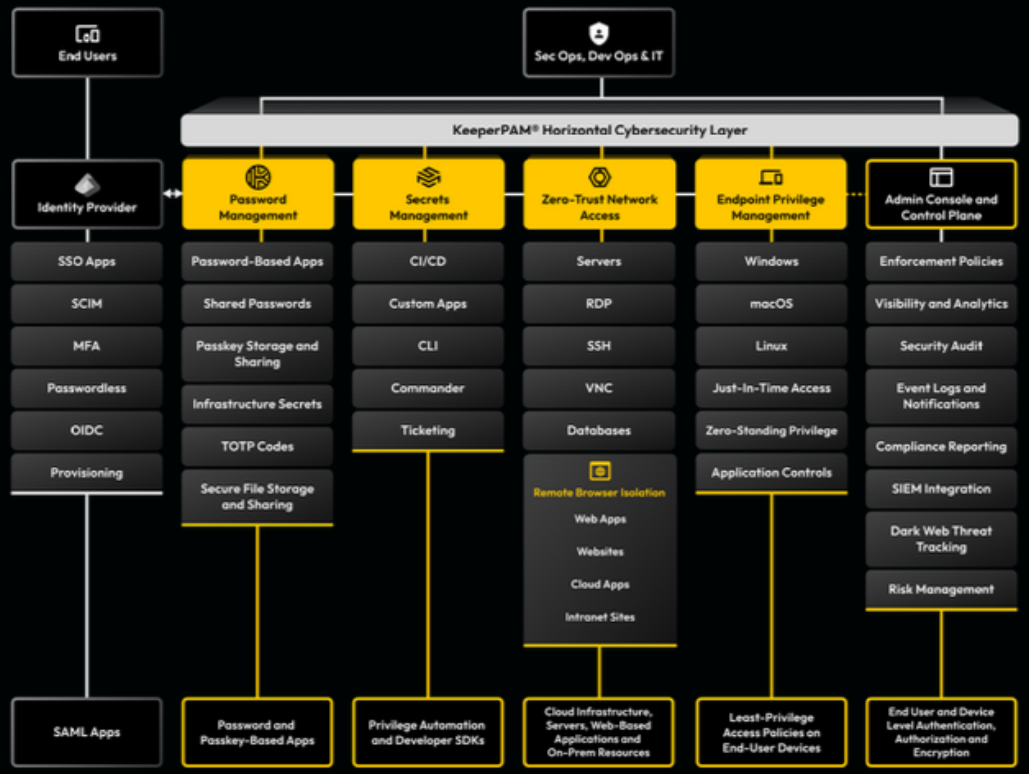
About Us

Keeper Security is transforming cybersecurity for people and organizations globally. Keeper's intuitive solutions are built with end-to-end encryption to protect every user, on every device, in every location. Trusted by millions of individuals and thousands of organizations, Keeper is the leader for password, passkey and secrets management, privileged access, secure remote access and encrypted messaging.

KEEPER®

KEEPER PASSWORD MANAGER

Keeper Privileged Access Management Platform



Business Value

- Prevent ransomware and credential-related cyber attacks
- Get comprehensive visibility, enforce security best practices and controls, and streamline compliance audits
- Enhance and extend your existing Single Sign-On (SSO) deployment
- Improve employee productivity and reduce the burden of password-related tickets for your helpdesk and IT teams

Key Capabilities

- Encrypted end-user vaults
- Password and passkey storage, management and sharing
- KeeperFill® browser extension powered by KeeperAI™
- Web, desktop and mobile apps
- Dark web monitoring with BreachWatch
- Seamless provisioning and integrations
- Role-Based Access Controls (RBAC)

KEEPER®

KEEPERPAM Sales Battlecard

What is KeeperPAM?

KeeperPAM™, a next-gen, zero-trust, zero knowledge solution, provides a simple, effective, easy-to-use and simple way to deploy a Privileged Access Management (PAM) tool that eclipses traditional PAM solutions. Keeper is the first company in the industry to unify three essential PAM products for unparalleled cost-effectiveness, rapid provisioning and ease-of-use. KeeperPAM includes:

- **Keeper Enterprise Password Manager (EPM)**
  Enables organizations to manage, protect, discover, share and rotate passwords with security, control and visibility to simplify auditing and compliance.
- **Keeper Secrets Manager (KSM)**
  Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.
- **Keeper Connection Manager (KCM)**
  Provides an agentless remote desktop gateway for instant privileged session management, remote infrastructure access and secure remote database access – without the need for a VPN with RDP, SSH keys, database and Kubernetes.

Why Did We Launch KeeperPAM?

According to a global research report, PAM users want a simple solution that is secure and fast to deploy. Some findings include:

- 87% of respondents say they would prefer a simplified form of PAM that is easier to deploy and use.
- On average, IT teams only use 62% of their current PAM functionality. 58% of respondents agree there is waste in their PAM solution.
- Roughly two-thirds of survey respondents indicate that pricey and superfluous PAM features create too much complexity for users, reducing user satisfaction.
- More than half of all IT teams – 56% – report they tried to deploy a PAM solution but never implemented it. Of those, 92% said it was because their PAM solution was too complex.
- Most organizations – 85% – say their PAM product requires dedicated staff to manage and maintain.
- Two-thirds of IT leaders – 66% – say they need a better PAM solution, but 58% say they do not have one because it is too expensive.

What are the Use Cases for KeeperPAM?

Password Management. Protect and manage your organization's passwords, metadata and files with encryption to protect against threat actors.

Password Sharing. Securely share passwords and sensitive information with users and teams.

Password Discovery. Scan and Identify accounts in on-premises and cloud environments, and convert them into managed records in the vault.

Password Rotation. Rotate passwords, keys and secrets on a scheduled basis or upon check-in to mitigate the risk of abuse or misuse.

Secrets Management for DevOps. Eliminate secrets sprawl by removing hard coded credentials from source code, and scripts – with no code changes.

Privileged Session Management. Securely and simply manage applications, systems, containers and databases for users, teams, and nodes for any user, 3rd-party or contract employee.

SSH Key Management. Manage and protect SSH keys and digital certificates across your tech stack, while ensuring your secrets, passwords and files are only available to authorized individuals.

Remote Infrastructure Access. Initiate simple, secure remote access with RDP and common protocols, without the use of a VPN.

Secure Remote Database Access. Administrators can provide direct database access to MySQL and other database types via SSH and RemoteApp – without having to share credentials.

Single Sign-On Security. Seamlessly and quickly strengthen SAML-compliant IdPs, AD and LDAP for quick and secure access to other solutions.

Zero-Trust Security. Strengthen your organization with zero-trust security and policies to ensure a clearly defined perimeter outside of the network.

Passwordless Authentication. Enable passwordless authentication for fast, secure access to applications for the ultimate frictionless login experience.

Credential Governance & Controls. Gain visibility, control, and security across the entire organization.

Industry Compliance & Reporting. Achieve industry compliance and audit reporting including SOX, FedRAMP StateRAMP, HIPAA, PCI and more to meet compliance mandates.

Key Challenges for Organizations

- An organization's infrastructure consists of both humans and machines which need to be protected.
- The traditional IT perimeter has vaporized due to distributed remote work and multi-cloud computing.
- The attack surface has exponentially increased with more sophisticated attacks on additional devices, credentials and secrets on remote networks.
- Traditional cybersecurity solutions are heterogeneous. Disparate, isolated software products provide inadequate visibility, security, reporting and control.
- Heterogeneous IT environments radically increase operating risk because they create critical security gaps which leave organizations vulnerable.
- Purchasing, deploying and managing disparate software is cost-prohibitive and does not protect against modern internal and external threats.

KEEPER®

KEEPER PAM Sales Battlecard

What are Traditional PAM Concerns?

Cost Prohibitive. Far more expensive product costs, maintenance and support.

Difficult to Provision. Technically complex to deploy, requires dedicated resources having an average deployment time of 6 to 18 months.

Difficult to Use. Antiquated UI and product manuals that are often > 1,000 pages create end-user complexity and confusion.

Opaque Visibility. Hindered by disparate, antiquated products that focus on IT staff – not the entire organization.

Inadequate Security. Traditional solutions are often not zero trust or zero knowledge and thus, cannot protect against modern threat vectors.

What are the KeeperPAM Advantages?

Cost Effective. Fewer products to purchase and easier for IT to manage with fewer people.

Fast Provisioning. Seamlessly deploys and integrates with any tech or identity stack – in a few hours.

Easy to Use. Unified admin console and modern UI for every employee on all device types – average training is less than 2 hours.

Pervasive Visibility. Simplifies auditing and compliance with organization-wide role-based access control, event logging and reporting.

World-Class Security. Keeper enables zero trust transformation and is zero knowledge, which relegates all encryption key management at the client.

Qualifying Questions

Are you currently using a PAM solution?

If yes

Have you fully deployed your PAM solution?

Do you use all the features?

Do you need a solution that is agentless?

How have users adopted this solution?

How long did it take to deploy the solution?

If no

What components of PAM are you looking for?

Can you explain your process for managing highly-privileged accounts?

How are you currently securing these accounts?

How do you manage passwords?

How do you manage secrets?

Do you have password rotation?

Do you have session management?

Do you have a way to manage connections?

Competitive Talking Points

- Zero-knowledge
- Zero-trust
- FedRAMP & StateRAMP certified
- PBKDKF2 encryption
- Elliptic Curve encryption
- Agentless and clientless
- No complexity, simple to use
- Includes only the features you need
- Fast and easy to deploy
- Simple pricing
- No implementation fees
- Reduced operational costs
- 50+ integrations
- Rated best password manager on all review sites
- Cloud-based secrets management
- Highest value-to-cost ratio

Additional Resources - Next Steps

KeeperPAM web page

KeeperPAM datasheet

Keeper Privileged Access Management research report

KEEPER®

KEEPER

Keeper Security Knowledge Sheet

For more information

Go to the Keeper Partner Portal

Email: partners@keepersecurity.com

Who is Keeper Security

Keeper is the leading provider of zero-trust privileged access management and enterprise password management software, trusted by millions of individuals and thousands of organizations. The platform seamlessly integrates with any tech stack to prevent breaches, ensure compliance and enable easy and secure access to resources.

What Keeper Offers

KeeperPAM® secures and manages access to an organization's critical resources, including servers, web apps, databases and workloads. Every user and device in the enterprise is authorized and authenticated with monitoring, threat tracking and reporting.

KeeperPAM, a patented cloud-native, zero-knowledge platform, integrates enterprise password management, secrets management, connection management, zero-trust network access and remote browser isolation into one easy-to-use interface. Keeper's enterprise password management solution is part of KeeperPAM, allowing organizations to deploy a unified platform and assign PAM licenses to users who require them, while providing enterprise password manager licenses to others.

Why Keeper Stands Out

Keeper is FedRAMP and StateRAMP Authorized, SOC 2 Type I and II compliant, and ISO 27001, 27017 and 27018 certified. Keeper has award-winning customer support and ranks highly in independent reviews. The solution is the only one of its kind in the industry, unifying traditional enterprise password management and PAM functionality in a simple, easy-to-deploy cloud platform that is cost-effective and highly secure.

Cybersecurity Statistics

82% Of IT leaders say they'd be better off moving their traditional PAM solution to the cloud

58% Of IT teams have not deployed a PAM solution because it was too expensive

68% Of breaches involve the human element, with the majority due to stolen or weak passwords, credentials and secrets

>70% Of phishing attacks aim to steal login credentials

Dangerous Employee Cybersecurity Habits

Reusing passwords – If just one reused password is compromised, every account that uses the same password is also at risk

Creating weak passwords – Weak passwords are easier for an unauthorized user to guess or crack

Resetting passwords multiple times – The more often you manually reset your passwords, the more likely you are to use weak passwords or begin reusing passwords if you don't use a password manager

Sharing passwords insecurely – Insecure sharing methods like text message and email are not encrypted, which means anyone can intercept them

Keeper's Zero-Trust, Zero-Knowledge Platform

- Monitors and protects every user on every device across the organization
- Seamlessly integrates with your existing IT stack
- Provides comprehensive authentication and encryption across every website, application and system employees interact with
- Consolidates enterprise password management and PAM functionality into a single interface
- Provides visibility, security and control of credentials across the organization

KEEPER®

Threat Briefing

Randy Hinders

August Threat Briefing Major News

- SharePoint OnPrem Targeted
  - Multi layered attack, using one vuln to bounce to another (common theme these days, see Apple update below)
  - Web Application Firewall / Gateways should be used for all end points. Never put the full server on the internet. It would have detected an initial request to the /toopane.aspx page and should have blocked the attack.

- Wordpress Exploit in the Wild
  - A plugin called "Alone - Charity Multipurpose Non-profit WordPress Theme" has a hole that will allow full access to the site just uploading a file and exploiting AJAX components. (https://thehackernews.com/2025/07/hackers-exploit-critical-wordpress.html)

August Threat Briefing Major News

- Possible ChatGPT Date Leakage
  - If you have ever shared a chat in ChatGPT, it might be indexed by Google. You can test this by searching Google for site:chatgpt.com/share GoCyber Collective
- Minnesota Hack Reported First on Slack
  - If you aren't yet in the slack group, you might want to consider it. We heard about this hack and the national guard being called up days before anyone else was talking about it.
- Sonic Wall VPN Issues Reported First on Slack
  - By now you should have your Gen7 SonicWall VPN offline, if not it might already be compromised.

August Threat Briefing
Major News

- Exchange Servers OnPrem & MS Teams Under Attack
  - Exchange should be behind a 3rd party spam/virus filter and never directly on the internet
  - MS Teams is fake Tech Support Social Engineering attack where they trick users into running a powershell script and gain local admin access.
- WinRAR is Being Exploited, Update ASAP
  - Hackers can override the "extract to" path and place malware In the startup or windows folders.

All kinds of Siemens and Rockwell industrial control systems need to be patched! If you run either, but sure to update.

August Threat Briefing
Major News

- Remember the United Healthcare Incident from Feb 2025?
  - 192.7 million people were impacted.
    - Largest Healthcare Incident to date!
- Speaking of Hacks... One of Google's salesforce instances was breached
  - 2.5 Million records, mostly Google Ad customer data
    - Guess how they got in.... Yep. Social engineering

August Threat Briefing: OS Updates

Apple Updates for Mac & iOS - https://thehackernews.com/2025/07/apple-patches-safari-vulnerability-also.html - The vulnerability, tracked as CVE-2025-6558 (CVSS score: 8.8), is an incorrect validation of untrusted input in the browser's ANGLE and GPU components that could result in a sandbox escape via a crafted HTML page." - How many people still click the 'sponsored links' on google search results?

Windows 11 Update – 130 Vulnerabilities Patched - Tweaks to "Windows Recall" are on the list (who uses that??)

August Threat Briefing: Must Reads

Google Releases Its H2 2025 Cloud Threat Horizons Report. Top 5 Items to Watch for Based on the Advanced Release:

1. **Foundational Security:** Credential compromise and misconfiguration remain the top entry points for threat actors in cloud environments. Foundational security measures are the most effective defense against these persistent threats.

2. **Targeting Backup Infrastructure:** Financially motivated threat groups are increasingly targeting backup systems, challenging traditional disaster recovery methods. This highlights the need for Cloud Isolated Recovery Environments (CIRE) to ensure business continuity.

3. **Social Engineering and MFA Bypass:** Advanced threat actors are using social engineering to steal credentials and session cookies, bypassing multi-factor authentication (MFA) to compromise cloud environments and steal high-value assets for financial gain.

4. **Decoy Files:** Threat actors are misusing trusted cloud services to deliver decoy files, such as PDFs from legitimate cloud storage, to infect systems. This tactic deceives victims while malicious payloads are downloaded in the background.

5. **Browser Extension Supply Chain:** To counter threat actors using compromised OAuth tokens to bypass MFA and inject malicious code, Google introduced Verified CRX Upload controls to secure the non-human identities used in cloud-based build processes.

September Speaker
Anna Blair – KBR

- Senior Systems Engineer
- Securing What Matters: A Systems Perspective on Cyber Risk
- How Safety Concepts Inform a Broader View of Security
- Proactively Reason Cybersecurity Beyond Component-Level Threats

August Parting Shots

- Local Gov't/Public Safety SIG – Sun Watch Room
- Education SIG – Wright Patt Room
- Defense Contractor SIG – Hawthorn Room
- Sponsorship Committee
- Turn in your lanyards at the desk

Information

Email me at john@GoCyberCollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register for future breakfast meetings from the website.

- GoCyberCollective.org

Event Sponsors

SECURECYBER™

Proven. Proactive. Personalized.

KEEPER®