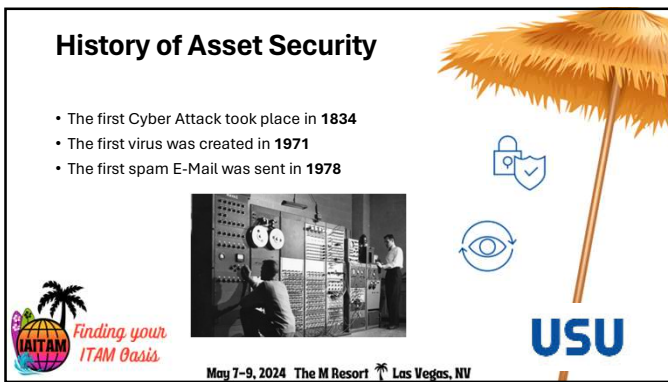




IAITAM ACE
 May 7-9, 2024 The M Resort Las Vegas, NV
 Robbie Plourde, USU
 Enhancing Asset Security in the Digital Age
 How ITAM can help Safeguarding Your Assets
 in an Evolving Landscape
Finding your IAITAM Oasis

1




History of Asset Security

- The first Cyber Attack took place in **1834**
- The first virus was created in **1971**
- The first spam E-Mail was sent in **1978**

Finding your ITAM Oasis
 May 7-9, 2024 The M Resort Las Vegas, NV
 USU

2



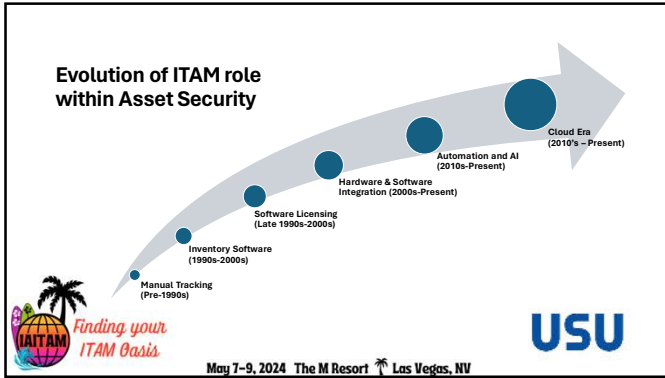
Emerging threats

Cyber threats to asset security are diverse and constantly evolving as technology advances. Some of the top cyber threats include:

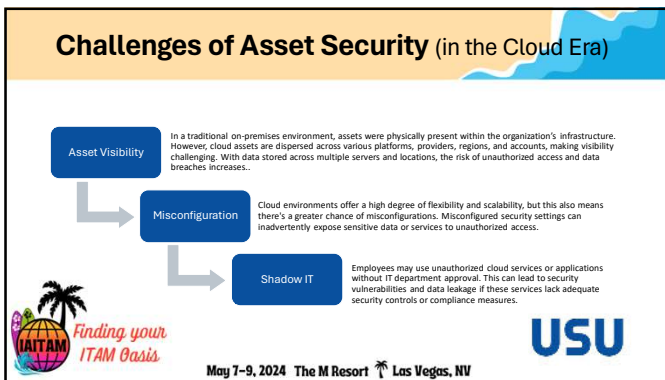
- Malware
- Phishing Attacks
- Data Breaches
- Ransomware
- Insider Threats
- Distributed Denial of Service (DDoS) Attacks
- Social Engineering

Finding your ITAM Oasis
 May 7-9, 2024 The M Resort Las Vegas, NV
 USU

3



4



5

Security has Never Been More Essential

The most successful Cybersecurity teams work with ITAM teams to ensure products are up to date, patches installed, end of support/life products removed, and other types of vulnerabilities identified.

However, according to IDG report, nearly 80% find it challenging to access the data needed to make sound decisions.

Difficulty Accessing Security-Critical Data

Category	Percentage
Extremely challenging	1%
Very challenging	20%
Somewhat challenging	21%
Not very challenging	47%
Not at all challenging	11%

Ability to collaborate by IT Security and IT Asset Management Teams

Category	Percentage
Communication only when risk is detected	10%
Some shared processes are in place to mitigate risk	43%
Highly collaborative with a unified risk mitigation strategy	41%

USU
 Finding your ITAM Oasis
 May 7-9, 2024 The M Resort Las Vegas, NV

6

Critical Importance of Trustworthy Data

- Trustworthy Data is the foundation of IT Asset Management according to ISO 19770-1
- "Trustworthy Data is data that is accurate, complete, relevant, readily understood by and available to those authorized users who need it to complete a task."
- Security, Procurement, IT Ops, Finance, FinOps, and ITAM all make decisions based on the same trustworthy data.

The goal is to combine and normalize data to generate rich data which can serve all stakeholders.

Framework for trustworthy data

USU

May 7-9, 2024 The M Resort Las Vegas, NV

Finding your ITAM Oasis

7

Why we should heed the warnings

- Less than 1% of organizations have visibility of at least 95% of their assets.
- Nearly 90% of device assets in the modern organization are cloud-based, meaning physical devices represent less than 10% of total devices.
- Only 45% of organizations have advanced asset intelligence with visibility and insight for over 75% of their assets.
- The average organization has well over 500 cyber assets for every human employee.
- 80% of organizations are pursuing a hybrid or multi-cloud strategy, and many organizations are experiencing cloud protection challenges.
- Difficulty coordinating activities among hybrid environments is the No. 1 challenge in understanding IT asset inventory.
- The average time to identify and contain a data breach is 277 days (about 9 months). —IBM
- The total number of annual cyber-attacks increased 38% in 2022, compared to 2021.

USU

May 7-9, 2024 The M Resort Las Vegas, NV

Finding your ITAM Oasis

8

Strategies - Enhancing asset security in the digital age

- Identify and Classify Assets
- Conduct Risk Assessment
- Implement Access Controls
- Update and Patch Systems
- Monitor and Detect Anomalies
- Stay Informed About Emerging Threats
- Security in the cloud
- Make known what ITAM can provide

USU


May 7-9, 2024 The M Resort Las Vegas, NV

Finding your ITAM Oasis

9

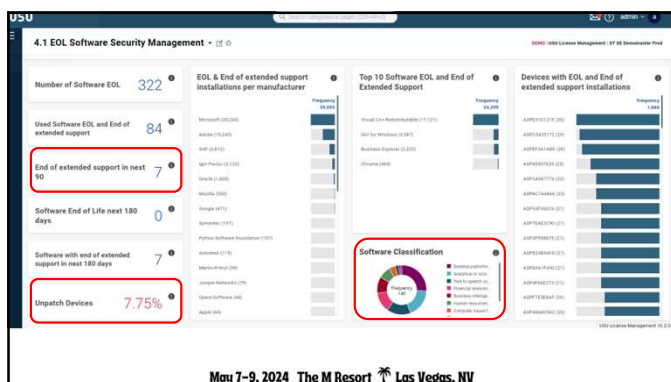
Identify and Classify Assets

- Begin by **identifying all assets** within your organization, including data, systems, applications, and devices.
- **Classify** these assets based on their sensitivity and criticality to prioritize security efforts.
- **Utilize automated tools and technologies** to discover and inventory assets across your organization's networks, systems, and cloud environments.
- Periodically review and **update your asset inventory** and data classification policies to reflect changes in your organization's infrastructure, technology landscape, regulatory environment, and business priorities.



May 7-9, 2024 The M Resort Las Vegas, NV

10




May 7-9, 2024 The M Resort Las Vegas, NV

11

Conduct Risk Assessment

- Perform a thorough risk assessment to **identify potential vulnerabilities** and threats to your assets.
- Evaluate the likelihood and impact of various security risks to determine **where** to focus your security efforts.
- Develop **risk mitigation strategies** and controls to reduce the likelihood and impact of identified risks to an acceptable level.
- Establish mechanisms for **ongoing risk monitoring**, measurement, and review to track changes in the risk landscape and assess the effectiveness of risk mitigation efforts.
- Foster a culture of **continuous improvement** by incorporating lessons learned from the risk assessment process into future risk management activities



May 7-9, 2024 The M Resort Las Vegas, NV

12

Number of vulnerabilities	Name (Item Name)	Severity (Risk Score)	Classification	Associated Microsoft Score (CVSS)	Number of Administrators	Owner Name
1	Active Mail Plugin (1) Plugin	11.0-9921-380	Runtime and browser ext	10.00	1	2023-03-11
1	Microsoft Office Professional Plus 2019	10.0-8422-1017	Productivity Suite	10.00	1	2023-01-08
1	Active Mail	9.7.0-1860	Runtime	10.00	1	2023-01-08
1	Active Mail	9.7.0-1860	Runtime	10.00	1	2023-01-08
1	Java(TM) SE Development Kit 8 Update 27 (8u27)	1.8.0-275	Software Development Kit	10.00	100	2023-12-19
1	Active Mailer 1.0.0	9.0.0	Document viewer	10.00	100	2023-09-01
1	Java(TM) 7 Update 80 (80)	7.0-80	Runtime Environment	10.00	1	2018-07-27
1	Active Mail Plugin (1) Plugin	10.0-0-001	Runtime and browser ext	10.00	1	2023-06-20
1	Active Mailer Reader (C) - Turkish	11.0.0-20063	Document viewer	10.00	1,027	2023-06-03
1	Apple	11.0-2-26	Media player	10.00	878	2023-11-29
1	Apple	11.0-2-26	Media player	10.00	168	2023-11-19
1	Java(TM) SE Development Kit 8 Update 21 (8u21)	1.8.0-210	Software Development Kit	10.00	168	2023-12-19
1	Java 7 Update 70 (8u69)	7.0-700	Runtime Environment	10.00	168	2011-07-27
1	MacOS Mailbox 10.0.0 (10A-010)	10.0.0	Browser	10.00	717	2017-08-27
1	Apple	7.0-700	Runtime Environment	10.00	168	2011-07-27
1	Active Mailer	10.0-0-001	Runtime	10.00	168	2023-06-20
1	Apple	9.0-0-200	Runtime Environment	10.00	200	2023-11-19

13

Implement Access Controls

- Establish robust user **identity management** practices, including user authentication, authorization, and account management.
- Use **Principle of Least Privilege (PoLP)** to restrict access to only those who need it to perform their job responsibilities.
- Implement **Role-Based Access Control (RBAC)** to assign permissions and access rights based on users' roles, responsibilities, and organizational hierarchy.
- Use strong authentication methods such as **multi-factor authentication (MFA)** to verify user identities and prevent unauthorized access.
- Provide **comprehensive training and awareness** programs to educate users about access control policies, best practices, and security awareness.

May 7-9, 2024 The M Resort Las Vegas, NV

14

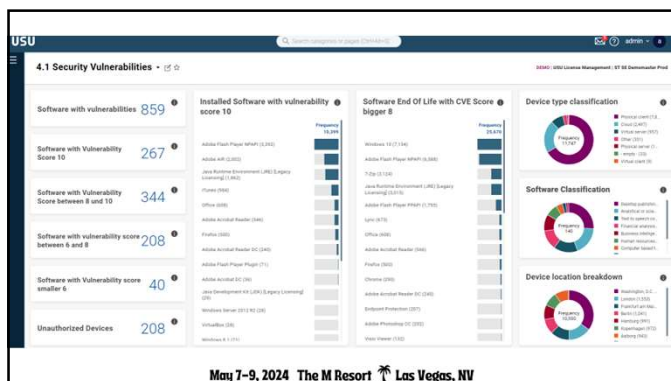
Update and Patch Systems

- Use automated scanning tools to **detect vulnerabilities** and prioritize patching efforts.
- Keep all software, operating systems, and firmware **up to date** with the latest security patches and updates.
- Regularly **patching known vulnerabilities** helps prevent attackers from exploiting weaknesses in your systems.
- Establish a **patch management policy** that outlines procedures, responsibilities, and timelines for updating and patching IT systems.
- Conduct regular vulnerability assessments and scans to **identify security vulnerabilities** in IT systems, applications, and infrastructure.

Educate users about the importance of updating and patching IT systems to mitigate security risks and protect against cyber threats.

May 7-9, 2024 The M Resort Las Vegas, NV

15



16

Monitor and Detect Anomalies and Vulnerabilities

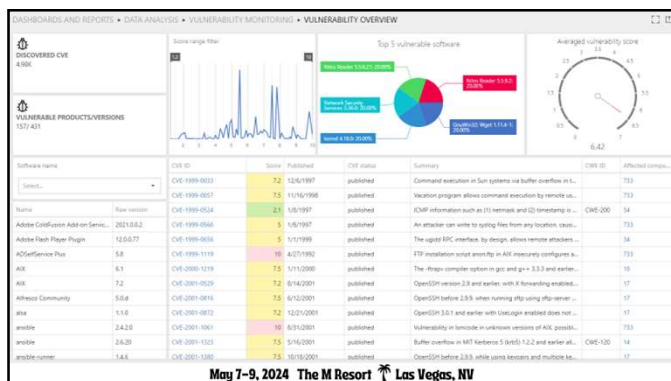
- Implement **continuous monitoring solutions** to detect and respond to security incidents in real-time.
- Use security information and event management (SIEM) tools to **aggregate and analyze** security logs for signs of suspicious activity.
- Establish **baseline patterns** of normal behavior for IT systems, networks, and user activities.
- Provide regular **security awareness training** to all employees to educate them about the importance of security and how to recognize and report potential security threats and anomalies.
- Continuously **review and update your monitoring and detection processes** to adapt to evolving threats and vulnerabilities. Regularly evaluate the effectiveness of your controls and make necessary adjustments.

ITAM Finding your ITAM Oasis

USU

May 7-9, 2024 The M Resort Las Vegas, NV

17



18

Stay Informed About Emerging Threats

- Subscribe to Industry Newsletters and Blogs
 - Krebs on Security -> <https://krebsonsecurity.com/>
 - Dark Reading -> <https://www.darkreading.com/>
 - The Hacker News -> <https://thehacknews.com/>
- Follow Security Thought Leaders on Social Media
 - Bruce Schneier: @schneierblog - renowned security technologist, author, and cryptographer.
 - Brian Krebs: @briankrebs - investigative journalist who covers cybersecurity, cybercrime, and technology security.
 - Troy Hunt: @troyhunt - Cybersecurity expert, and the creator of the "Have I Been Pwned?" breach notification service.
 - Nicole Perleth: @nicoleperleth - Cybersecurity journalist for The New York Times
- Join Online Communities and Forums
- Monitor Vulnerability Databases and Threat Feeds
 - National Vulnerability Database (NVD)
 - Common Vulnerabilities and Exposures (CVE)
- Engage in Continuous Learning and Professional Development

May 7-9, 2024 The M Resort Las Vegas, NV



19

Stay Informed About Emerging Threats

Emerging technologies will exacerbate long-standing challenges related to cyber resilience.

In the next two years, will generation Z perceive social cyber challenges to be greater or smaller?

Greater	58.8%
Smaller	38.1%
Don't know	3.1%

What are you most concerned about in regards to generative AI input/output?

Malicious use of AI	45.2%
AI-powered phishing	38.5%
AI-generated deepfakes	32.1%
AI-powered malware	28.7%
AI-powered social engineering	25.3%
AI-powered identity theft	22.9%
AI-powered fraud	20.4%
AI-powered data breaches	18.6%
AI-powered ransomware	16.8%
AI-powered supply chain attacks	14.2%
AI-powered insider threats	12.5%
AI-powered zero-day exploits	10.7%
AI-powered botnets	9.3%
AI-powered DDoS attacks	8.1%
AI-powered spam	7.4%
AI-powered malware distribution	6.2%
AI-powered social media manipulation	5.5%
AI-powered data mining	4.8%
AI-powered surveillance	3.9%
AI-powered identity verification	3.1%
AI-powered fraud detection	2.4%
AI-powered security testing	1.8%
AI-powered threat intelligence	1.2%
AI-powered incident response	0.9%
AI-powered digital forensics	0.6%
AI-powered network monitoring	0.4%
AI-powered system administration	0.3%
AI-powered user experience	0.2%
AI-powered customer support	0.1%

AT&T data breach leaks info of 7.6M customers to dark web

2. Ransomware attack on key US and UK water companies


Two major water utility companies in the US and UK have been targeted by separate ransomware attacks resulting in apparent data breaches, Security Week reports.

Finland Blames Chinese Hacking Group APT31 for Parliament Cyber Attack

May 10, 2024 Cyber Strategy - Helsinki

The House of Finland's Cyber Intelligence Centre reported Chinese hackers who hacked an MP for the parliament in a cyber...

May 7-9, 2024 The M Resort Las Vegas, NV



20

Security in the cloud

- Adopt a Zero Trust security model
- Implement robust Identity and Access Management (IAM) controls to manage user identities, permissions, and access to cloud resources.
- Encrypt sensitive data both in transit and at rest.
- Leverage built-in security services provided by cloud service providers, such as AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center.
- Implement continuous monitoring solutions to track user activities, configuration changes, and security events in real time.
- Establish governance policies and procedures to enforce security, risk management, and data protection practices across cloud environments.

Foster collaboration and information sharing with your secur

May 7-9, 2024 The M Resort Las Vegas, NV



21

How to promote better collaboration - ITAM and Cybersecurity

According to the IDG report, 59% report their IT security and IT asset management teams are lacking a unified risk mitigation strategy.

- Create an advisory group with the goal of sharing information about strategy, plans, projects, goals, and objectives.
- It may be advantageous to bring both functions into a common governance framework
- Ultimately, collaboration between Cybersecurity and ITAM teams benefits all areas of the organization.

Only 34% highly collaborate. Not surprisingly, this issue seems to compound the larger an organization is, with only 34% of enterprise organizations (50,000 users and more) indicating they are highly collaborative.

IT Endpoints	Highly Collaborative
2,000 - 9,999 IT endpoints	46%
10,000+ IT endpoints	34%

Finding your ITAM Oasis

May 7-9, 2024 The M Resort Las Vegas, NV

22

Things to remember and review

- Asset Inventory and Classification
- Access Control and Privilege Management
- Data Encryption
- Patch Management & Endpoint Security
- Implement security awareness
- Continuous Monitoring & Threat Detection
- Security Culture and Governance
- Emerging Technologies and Trends

Finding your ITAM Oasis

May 7-9, 2024 The M Resort Las Vegas, NV

23

Robbie Plourde
Principal Solution Engineer
FinOps Certified Practitioner
+1 (757) 525.0075
Robbie.plourde@usu.com
www.usu.com

Finding your ITAM Oasis

May 7-9, 2024 The M Resort Las Vegas, NV

24
