IAITAM ACE 2025

ITAM - Another Brick In The Wall

Proactive Cybersecurity

For SAM & HWAM Practitioners

BELARC

Agenda

- Basic cybersecurity terms
- Proactive vs reactive cybersecurity
- Defenders can have an advantage
- Does proactive cybersecurity work?
- Case study: US National Security Agency, Center for Internet Security
- How SAM & HWAM can help
- Example controls in action
- Q&A and Lessons Learned from the audience

Basic cybersecurity terms

- Attack
  - Unauthorized attempt to access, change, or destroy data, applications or systems.
  - Objectives: steal money or data, disrupt business.
- Breach
  - Successful attack.
  - Unauthorized access to confidential info, loss of access to IT assets.
- Control
  - Measure that protects IT assets from cyber attacks becoming breaches.
  - Technical, Process, Management

Reactive cybersecurity

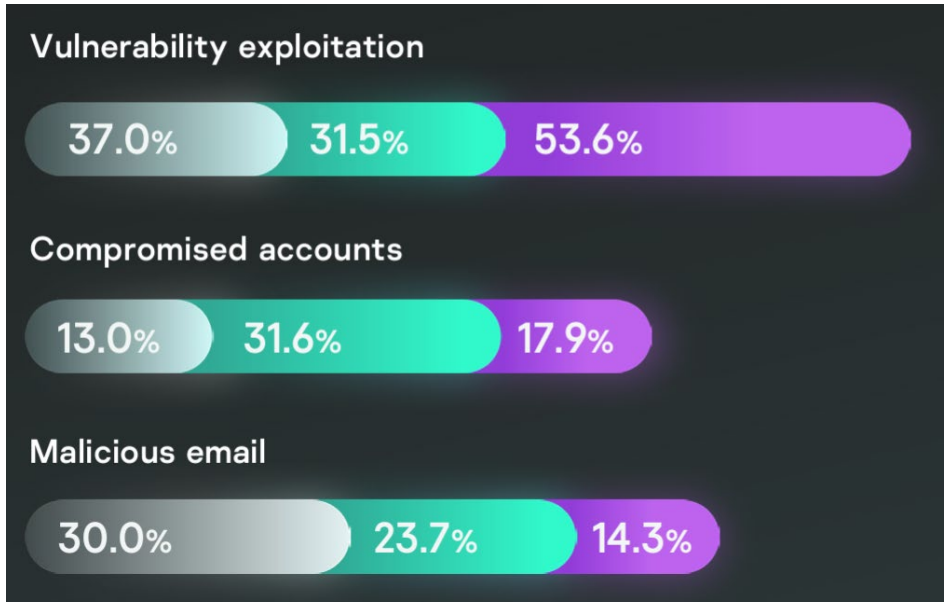
- Identifying breach after the fact.
  - Endpoint Detection & Response (EDR)
    - Monitors endpoints for suspicious activity
    - Crowdstrike, SolarWinds
  - Intrusion Detection Systems (IDS)
    - Monitors network traffic for suspicious activity
    - Checkpoint, Fortinet
  - Log monitoring systems
    - Analyze system logs for suspicious activity
    - Splunk, SolarWinds
- Reactive cybersecurity is often the main focus.
  - Stopping attackers in their tracks is exciting.

Proactive cybersecurity

- Security controls that prevent attacks from becoming breaches.
  - Center for Internet Security (CIS)
  - NIST 800-53
  - CMMC requirements – NIST 800-171
- Proactive cybersecurity is often neglected.
  - Not exciting.
  - No AI ☺).

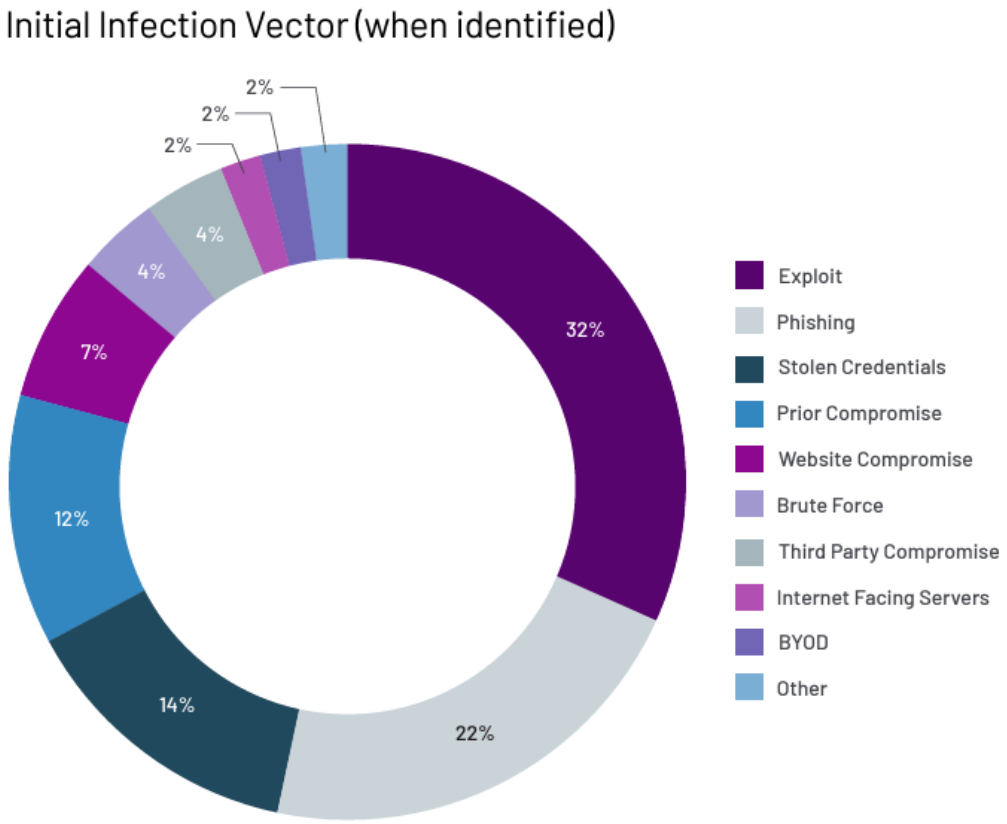
Defenders have an advantage - if we implement proactive controls

- Kaspersky “The nature of cyber incidents 2022”

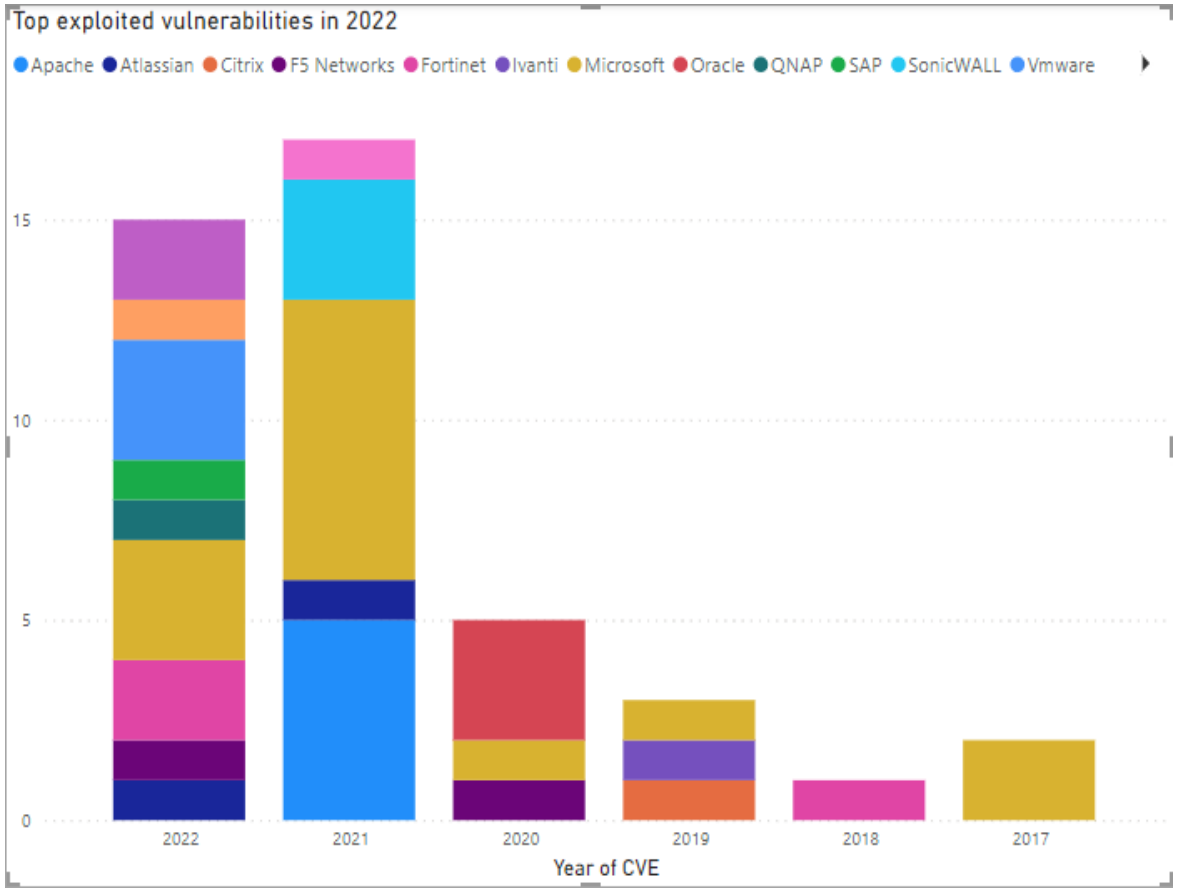


Defenders have an advantage

- Mandiant M-Trends 2023

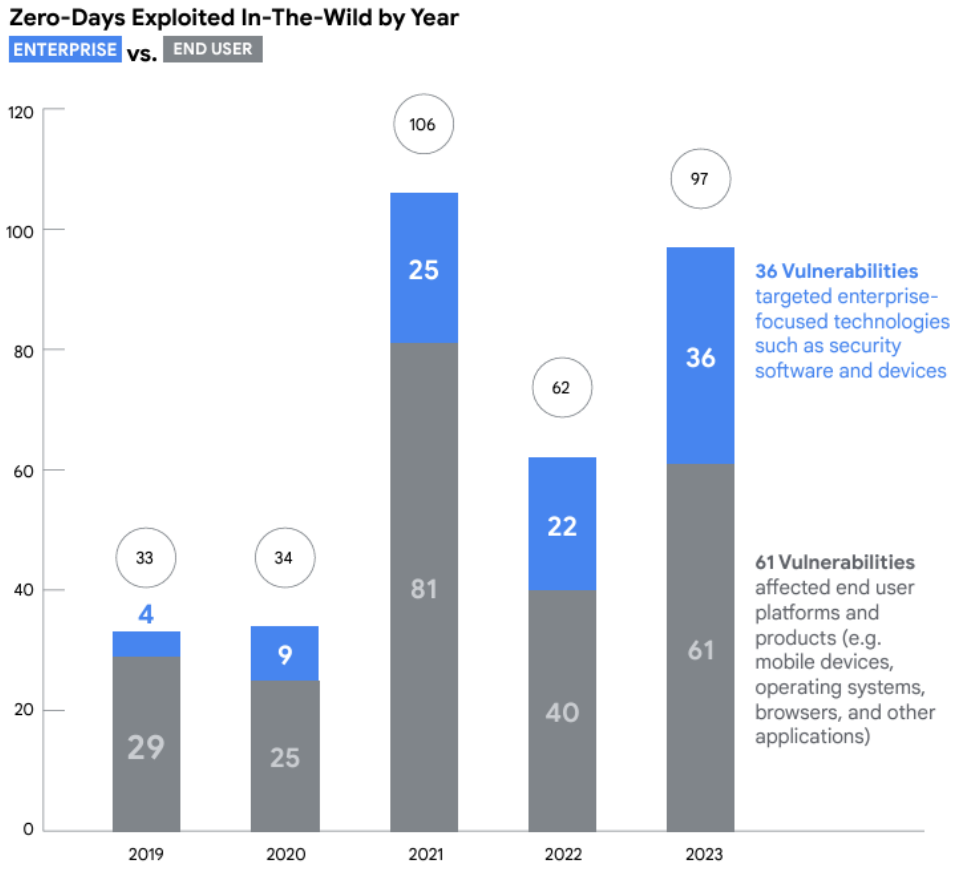


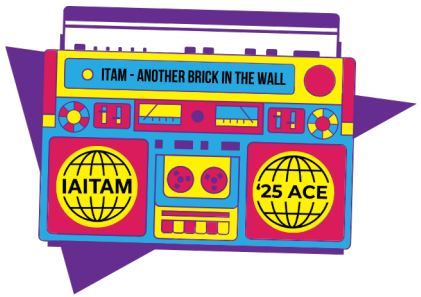
Top exploited vulnerabilities in 2022



Year	Total CVEs	Percent
2022	15	34.88
2021	17	39.53
2020	5	11.63
2019	3	6.98
2018	1	2.33
2017	2	4.65
Total	**43**	**100.00**

What about zero days?





BELARC

Does proactive cybersecurity work?

- NSA IAD under Tony Sager and Curt Dukes.
  - Responsible to defend US DoD from cyber attacks.
  - Red Team and Blue Team lessons learned.
    - Same attack vectors successful time after time.
  - Result: Defined cyber security controls within DoD
  - DoD and its contractors have gotten much better
    - Since the SecDef's Exchange Server breach and F-35 design data loss.
    - Cybersecurity Maturity Model Certification (CMMC).

Does proactive cybersecurity work?

- Center for Internet Security
  - Initially funded by NSA to impart lessons learned to industry.
    - CIS Controls. Now v8.1
  - SAM can help with Implementation Group 1 (IG1), or basic controls.
  - Basic controls (IG1) successfully defends against
    - 77% of top 5 attack types
    - 74% all attack types
    - Based on analysis of actual breaches.

CIS analysis of attacks and breaches

Top 5 Attacks	IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques	All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Privilege Misuse	86%	90%
Targeted Intrusions	83%	95%

Where SAM and HWAM can help

- CIS Critical Security Controls v8.1 – August 2024 (Top 7)
  - 1-Inventory and Control of Enterprise Assets (hardware & devices)*
  - 2-Inventory and Control of Software Assets*
  - 3-Data Protection*
  - 4-Secure Configurations of Enterprise Assets and Software*
  - 5-Account Management (manage credentials)*
  - 6-Access Control Management (MFA and user privileges)
  - 7-Continuous Vulnerability Management*
- * SAM and HWAM input on these IG1 Controls.
  - Requires accurate, complete and up-to-date data.

CIS controls example - Hardware

Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Asset Type: Devices	Security Function: Identify	IG1	IG2	IG3

Safeguard 1.2: Address Unauthorized Assets

Asset Type: Devices	Security Function: Respond	IG1	IG2	IG3

CIS controls example - Software

Safeguard 2.1: Establish and Maintain a Software Inventory

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Safeguard 2.2: Ensure Authorized Software is Currently Supported

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Safeguard 2.3: Address Unauthorized Software

Asset Type: Software	Security Function: Respond	IG1 IG2 IG3

CIS controls example – Data Protection

Safeguard 3.2: Establish and Maintain a Data Inventory

Asset Type: Data	Security Function: Identify	IG1	IG2	IG3

Safeguard 3.6: Encrypt Data on End-User Devices

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

CIS controls example – Account Management

Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Asset Type: Users	Security Function: Identify	IG1	IG2	IG3

Safeguard 5.3: Disable Dormant Accounts

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

CIS controls example – Vulnerability Management

Safeguard 7.3: Perform Automated Operating System Patch Management

Asset Type: Software	Security Function: Protect	IG1	IG2	IG3

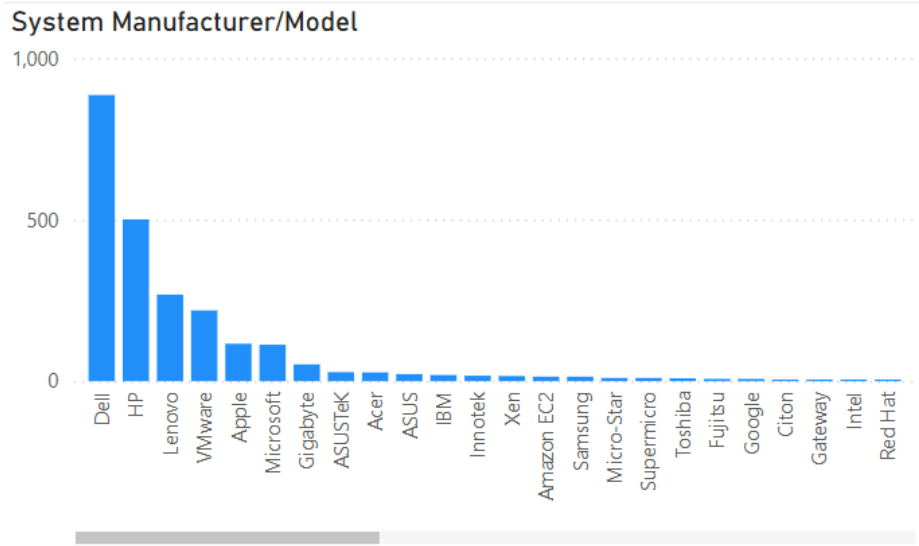
Safeguard 7.4: Perform Automated Application Patch Management

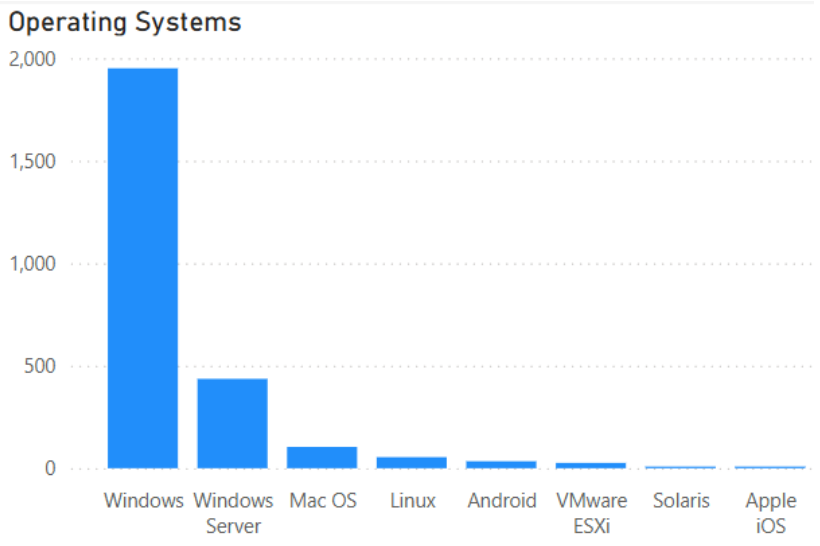
Asset Type: Software	Security Function: Protect	IG1	IG2	IG3

Example controls in action

- Data requirements
  - Accurate, complete and up-to-date
  - Able to be easily shared with other groups
  - Able to be easily used in workflow automation

Hardware assets

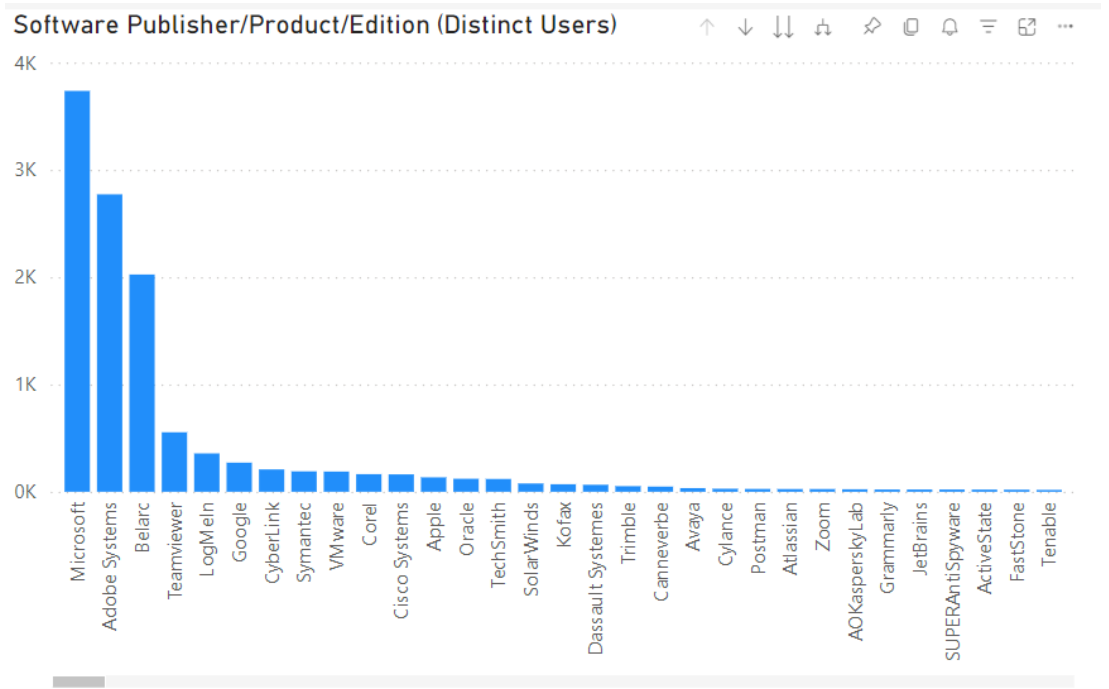




MachineClass	P	V	Total
Notebook	824		**824**
Notebook Server	2		**2**
Server	249	245	**494**
Workstation	1208	90	**1298**
Total	**2283**	**335**	**2618**

MachineClass	Android	Apple iOS	Linux	Mac OS	Solaris	VMware ESXi	Windows	Windows Server	Total
Notebook	25	1	2	79			717		**824**
Notebook Server								2	**2**
Server			19		7	26	8	434	**494**
Workstation	9	5	33	25			1226		**1298**
Total	**34**	**6**	**54**	**104**	**7**	**26**	**1951**	**436**	**2618**

Approved software



Software not used for X days

-1 6916

License Required?

- [ ] no
- [ ] yes

Non-compliant software

Noncompliant Software Versions

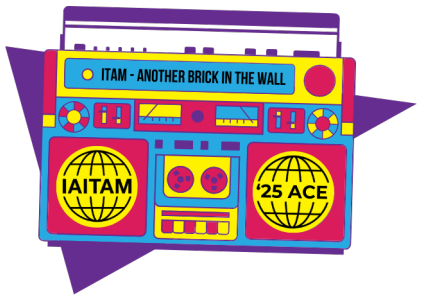
Note: The lowest compliant versions shown are for DEMO PURPOSES ONLY.
With a licensed copy of BelManage, your BelManage administrator can enter compliant versions of software on an administration page.

Summary of Group acme\ and its Subgroups

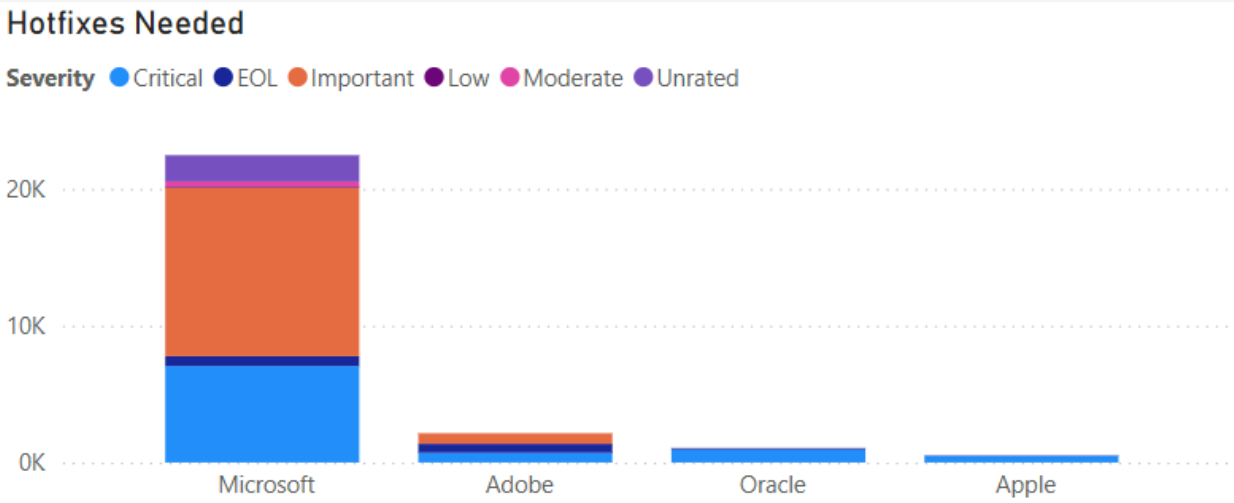
(Click a product name to see systems using a noncompliant version of that product)

Software Manufacturer

Systems	Product Name	Type	Range of Noncompliant Versions	Compliance Version Ranges
Adobe				
3	Acrobat	Windows	11.0.20.17 — 25.1.20428	20.5.30574 — 25
2	Acrobat DC	Windows	25.1.20428	20.5.30636 — 20.999, 24.2.20759 — 24.999
Atlassian				
1	Sourcetree	Windows	3.4.7	3.4.22 — 99
Don HO				
3	Notepad++	Windows	8.1.9 — 8.4.8	8.5.7 — 99
TechSmith				
1	Snagit	Windows	18.2.6.6375	24.1.2 — 25
The Git Development Community				
1	Git	Windows	2.33.1.1	2.47.1.2 — 99



Hotfixes needed & EOL software

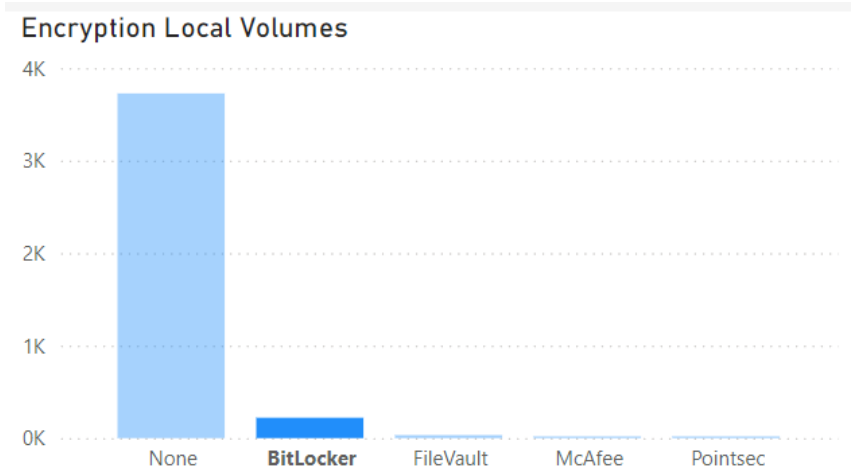


Vendor	Critical	EOL	Important	Low	Moderate	Unrated	**Total**
Adobe	714	654	773				**2141**
Apple	484	37					**521**
Microsoft	7053	713	12319	86	364	1919	**22454**
Oracle	951	98					**1049**
Total	**9202**	**1502**	**13092**	**86**	**364**	**1919**	**26165**

Hotfixes Needed

Computer	Name	BulletinId	QNumber	Severity	Vendor	Version	Description
desk_1880	EOL-Microsoft			EOL	Microsoft	Windows 2000	
srv_231	EOL-Microsoft			EOL	Microsoft	Windows 2000	
nb_1516	EOL-Microsoft			EOL	Microsoft	Windows 7 RTM	

Drive encryption



Encryption Local Volumes

Computer	User	Encryption
nb_692	1002	BitLocker
nb_1390	1007	BitLocker
nb_468	102	BitLocker
nb_1786	1021	BitLocker
nb_2067	1022	BitLocker
nb_56	1023	BitLocker
desk_1664	1037	BitLocker
nb_1385	1045	BitLocker
nb_1203	1054	BitLocker
desk_1393	1060	BitLocker
Total		

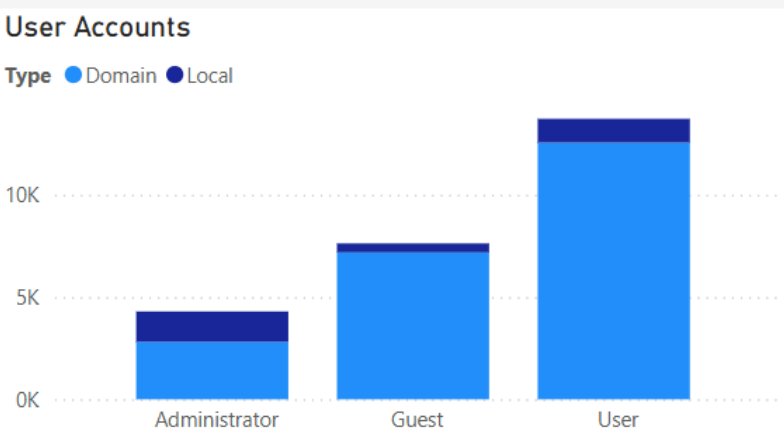
Encryption Suspended

- [ ] (Blank)
- [ ] no
- [ ] yes

Local Volumes

220

User accounts

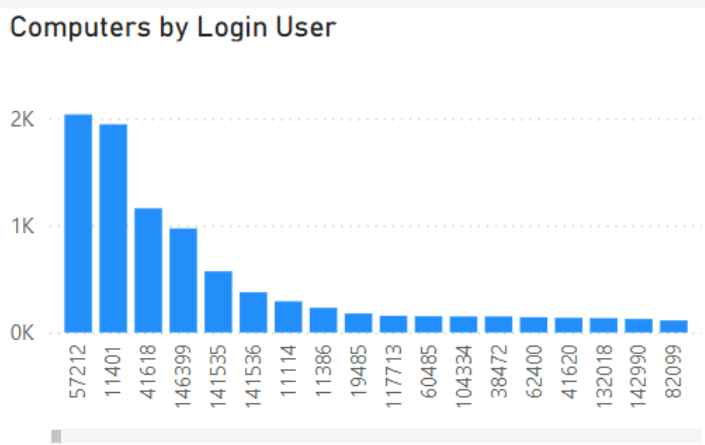


User Accounts

Type	Administrator	Guest	User	Total
Domain	2810	7181	12551	**21387**
Local	1485	442	1164	**2940**
Total	**4114**	**7608**	**13510**	**23786**

Password Age more than X days

0 11790



User Accounts

LoginUser	FullName	Privilege	Type	Computer	Email	Logins	LastLogin	AccountDisabled	AccountLockedOut	SID
100481		User	Domain	srv_1871	100481@abcxyz.com	1		no	no	784678283-153461445-2238456313-4617
100482		User	Domain	srv_2096	100482@abcxyz.com	1		no	no	2643922949-668658206-326545761-5293
100483		User	Domain	srv_2053	100483@abcxyz.com	1		no	no	940645971-1032339507-1231754661-4712
100490		User	Domain	srv_1871	100490@abcxyz.com	1		no	no	784678283-153461445-2238456313-4618
100499		User	Domain	srv_1807	100499@abcxyz.com	1		no	no	1896471786-1675500547-1460340569-5549
100499		User	Domain	srv_1808	100499@abcxyz.com	1		no	no	1896471786-1675500547-1460340569-5549

How SAM & HWAM can help insure cybersecurity

- Support your organization's cybersecurity controls effort
  - With accurate, complete, up-to-date data.
  - Controls can be CIS, NIST, home grown, etc.
- Integrate this data with Workflow Automation
  - Automate implementing and confirming the security controls.

Belarc company

- Over 1,800 customers worldwide
  - Commercial
    - Autodesk, Novelis (Canada, Korea), Shell Canada, Travelers Insurance (India)
  - US Federal Government
    - Environmental Protection Agency, Federal Aviation Administration, NASA, Patent & Trademark Office, Department of State (DS), US Air Force (844th CG)
  - Many long term >10 years
  - Located in 50 countries
- Eight US and Worldwide Patents

Q&A + Lessons Learned from you

Sumin Tchen

Belarc, Inc.

(e) stchen@belarc.com

info@belarc.com

www.belarc.com