Cybersecurity & the SAM Manager

Sumin Tchen

BELARC

Today's Topics

- Is SAM a Data Provider or Data Requestor
  - Which is more influential?
- What are Cybersecurity Controls
  - A little history
  - Do cybersecurity controls work?
  - Example controls
- Cybersecurity Controls and SAM
  - Sample reports
  - Recommendations

BELARC

Is SAM a **Data Provider** or a **Data Requestor**?

- Guess which one has more influence?
- Typical Data Providers:
  - Operations: SCCM/Jamf/Linux tools.
  - Human Resources: Identify employees, contractors, business units, managers, locations.
  - Finance: Purchase records, contracts

BELARC

Is SAM a **Data Provider** or a **Data Requestor**?

- Typical Data Requestors:
  - SAM
  - HWAM
  - Cybersecurity
  - Vendor management
  - Business Units

Why should SAM become a Data Provider?

- Data from Operations is not detailed enough for SAM
  - SAM needs software versions, editions, actual usage, SaaS usage.
  - Not normalized.
- Need an easy way to link this to HR data
  - Employee ID, manager, location.
- Data from Finance not regularized or normalized.
  - Software purchase and contract data
  - Needs to be in separate fields, i.e. Vendor, Product, Version, Edition.
  - Needs to be normalized.

Why should SAM become a Data Provider?

- SAM needs accurate, complete and up-to-date data
  - In the right form and detail.
- SAM can then share this data with others:
  - Cybersecurity, Vendor Management, Operations, Finance, Business Units.

What are Cybersecurity Controls?

- Processes, people and tools to reduce breaches of computer systems.
  - Breach = successful attack
  - Reduce the risk, not eliminate
- A little history: In the Dark Ages, i.e. 15-20 years ago
  - DoD required scans of networks once every three months.
  - FISMA requirements for Federal Gov is an annual checklist.
  - Checklists only, no actual verifications.
  - Commercial and DoD contractors developed their own processes.
  - No audits or verifications done.

BELARC

What were the results? Just some examples.

- Office of Personnel Management breach (2015)
  - 20 million detailed security clearance records stolen
  - 4 million personnel records
  - 5 million fingerprint records
- F-35 design data stolen from DoD contractor (2008)
- Secretary of Defense email server breach
- Adobe source code
- Many financial institutions, i.e. Experian (2015)

BELARC

What was done

- National Security Agency, Information Assurance Directorate (NSA IAD)
  - Responsible for defending DoD computer systems
  - Tony Sager, Director NSA IAD
    - Red team & Blue team same breach results year after year.
    - Some history: https://www.youtube.com/watch?v=SyLSA8kxV8Q
  - Resulted in consistent verifiable security controls for DoD
    - Security Technical Implementation Guides (STIGs)
  - Sponsored Center for Internet Security (CIS) for the public.

What was done

- US Government takes lead
  - Controls, listing of vulnerabilities - used by everyone including commercial, financial, foreign
- NIST tasked with developing controls & enumerating vulnerabilities
  - SP 800-53, SP 800-171
  - National Vulnerability Database (NVD), CVEs, CPEs, CVSS
- Cybersecurity and Infrastructure Security Agency (CISA) 2018
  - Part of DHS
  - Government (non-DoD), commercial, industrial
- Is this enough?
  - Based on the number of breaches, maybe not.
  - Commercial is voluntary. No disclosure requirements.

Example cybersecurity controls

- NIST: US Federal Government.
  - Detailed technical, process, and management controls.
- CIS: Originally from the NSA.
  - CIS Top 20 Controls. Prioritized, proven controls.
- ISO 27001: Process and management controls.
- UK National Cyber Security Centre: Basic top 5 controls.
- We will focus on the Technical Controls
  - vs the Process and Management Controls.

BELARC

Cybersecurity controls

- NIST SP 800-53, 800-171 controls
  - SP 800-53 are cybersecurity controls required for government.
    - Adopted by commercial, financial, industrial IT and OT.
  - SP 800-171 are a sub-set
    - Used by Federal Government and DoD contractors and suppliers.
    - Cybersecurity Maturity Model Certification (CMMC) for DoD contractors.
- CIS controls
  - Spinout of the NSA
  - Now focused on state and local governments.
  - CIS Top 20 Controls.

NIST Cybersecurity Framework

Cybersecurity controls, do they work?

- “All US Federal Government security breaches over the past two years have been caused by known security vulnerabilities” – Curt Dukes, Director IAD NSA
  - So why is the industry so focused on zero day attacks?
  - Cybersecurity tools vendors focus on shiny new objects: AI, Machine Learning
- CIS: Top 5 will reduce risk of breach by 85%, all 20 by 94%
- Today this focus on basic controls is known as “Cyber Hygiene”

BELARC

NIST controls and SAM

- System component inventory
  - “...system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.”
- Baseline configurations and changes
  - Software, hardware security configurations.
- Account management
  - Privileged User Accounts, Atypical Usage, Inactive accounts

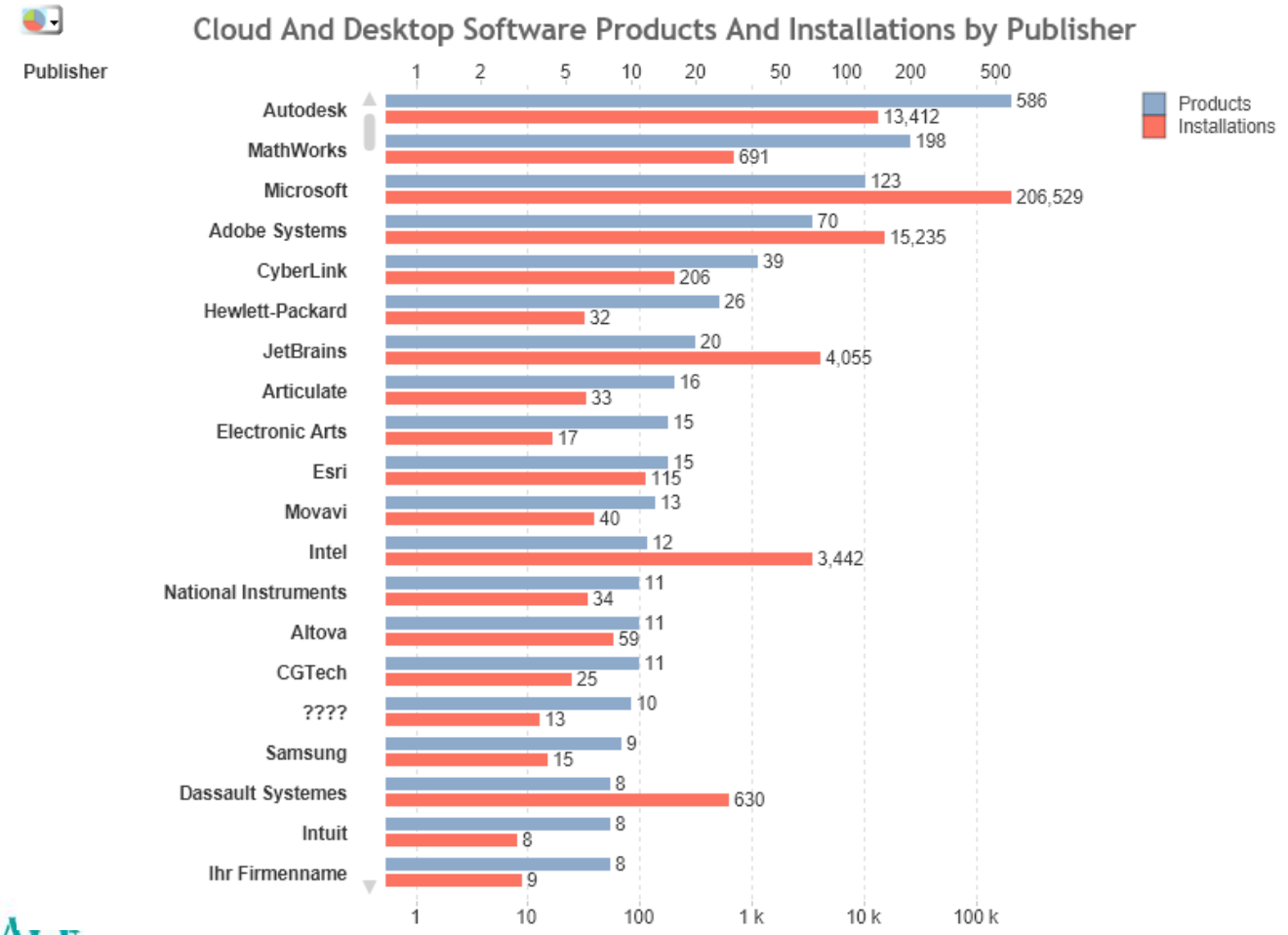
NIST controls and SAM

- Software usage
- User installed software
- Configuration change control
- Vulnerability monitoring
  - Including EOL software
- Continuous monitoring
- Ask for “Belarc Mapping to NIST controls” document for details.

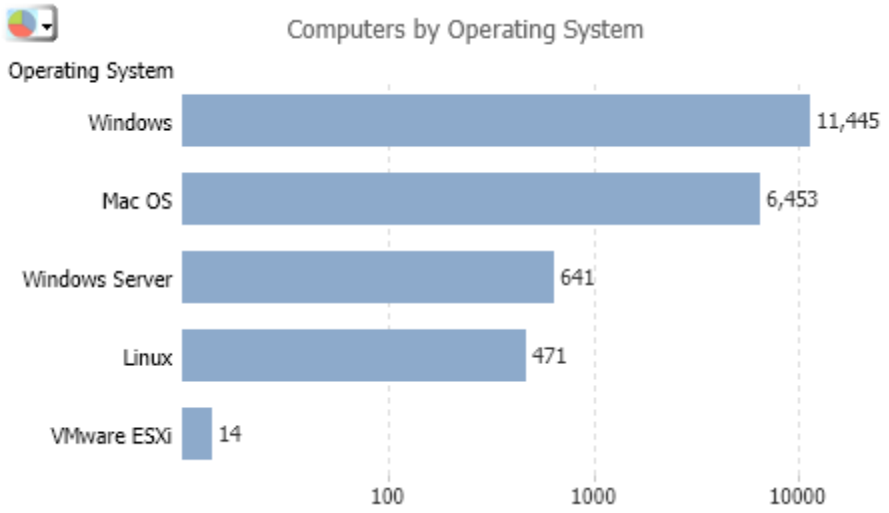
CIS controls and SAM

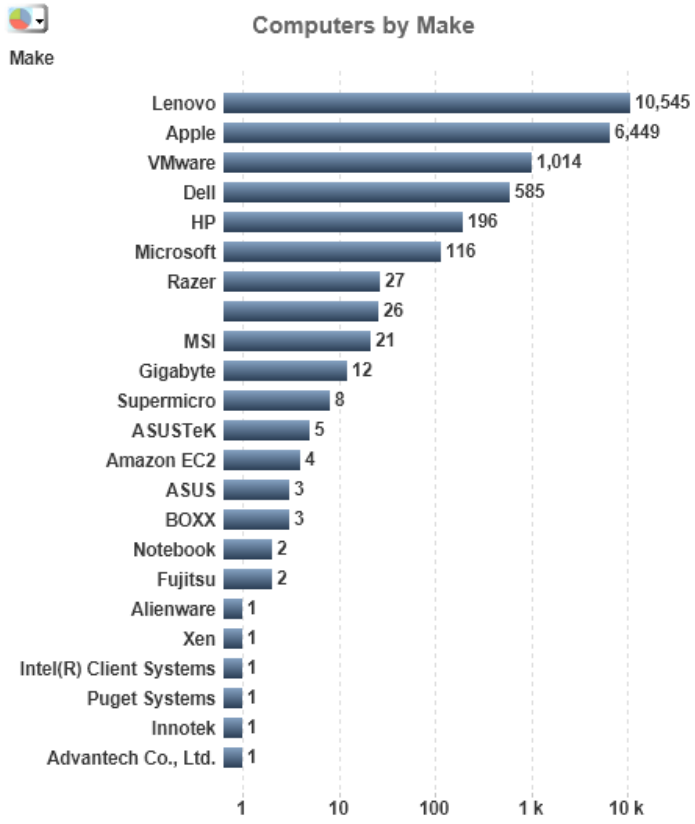
- CIS Top 5 controls: (out of 20)
  - Inventory of authorized and unauthorized **devices**
  - Inventory of authorized and unauthorized **software**
  - Controlled use of **admin privileges**
  - Continuous **vulnerability assessment** & remediation
  - Secure **configurations** for all devices
- Top 5 will reduce risk of breach by 85%, all 20 by 94%

Sample reports: Software



Sample reports: Hardware

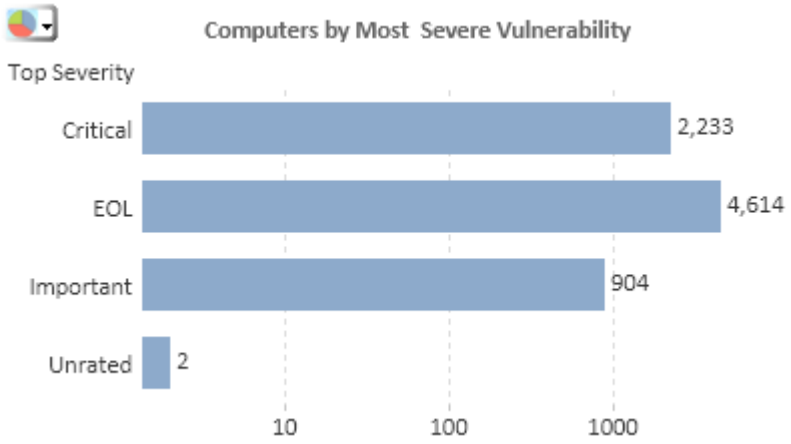




Adobe usage example

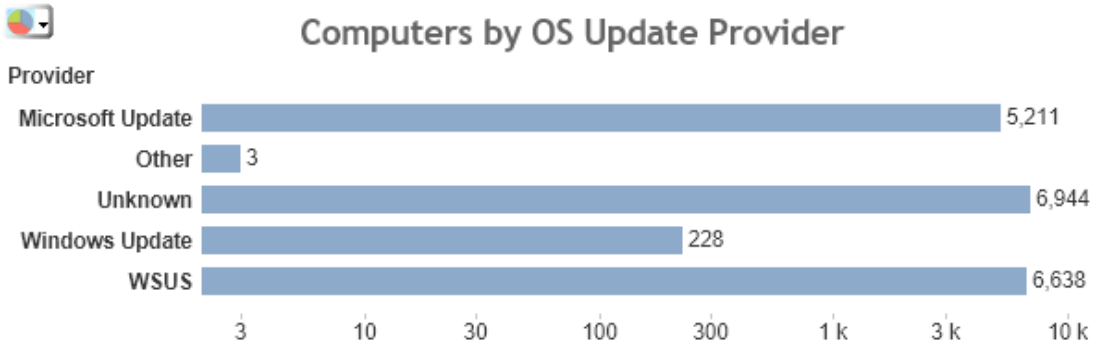
S I Status	Computer	User	Email	Product	Edition	Version	License Type	Last Used Date (By Computer)	Last Used Days Ago (By Computer)	Last Used Date (By User)	Last Used Days Ago (By User)	Install Date
S A I	desk_1004	11401	bdpym.fmpchj@...	Illustrator	None	CS6	cloud user	5/23/2021	500	5/23/2021	500	5/24/2017
S A I	desk_1146	11401	bdpym.fmpchj@...	Illustrator	None	2015	cloud user	10/10/2021	360	10/10/2021	360	3/30/2016
S A I	nb_985	23913	yewadx.vlkxlnh...	Acrobat	Pro DC T	2018	cloud user	10/13/2021	357	10/13/2021	357	4/12/2018
S A I	nb_985	23913	yewadx.vlkxlnh...	InDesign	None	CS6	cloud user	11/17/2021	322	11/17/2021	322	5/17/2018
S A I	nb_985	23913	yewadx.vlkxlnh...	Photoshop	None	CS6	cloud user	11/23/2021	316	11/23/2021	316	5/23/2018
S A I	desk_2290	142990	dhjwzo.qjjetq@...	Photoshop	None	CS3	cloud user	12/21/2021	288	12/21/2021	288	12/22/2019
S A I	nb_449	23248	wavagd.svbgwlv...	Captivate	None	11	cloud user	1/13/2022	265	1/13/2022	265	1/14/2020
S A I	nb_449	23248	wavagd.svbgwlv...	Creative Cloud All Apps Pro	Enterprise	2020	cloud user	2/26/2022	221	2/26/2022	221	2/13/2020
S A I	desk_387	25217	vaar.afhh@ucw...	Acrobat	Pro DC T	2020	cloud user	4/19/2022	169	4/19/2022	169	2/16/2020
S A I	desk_387	25217	vaar.afhh@ucw...	Creative Cloud All Apps Pro	Enterprise	2020	cloud user	4/27/2022	161	4/27/2022	161	2/16/2020

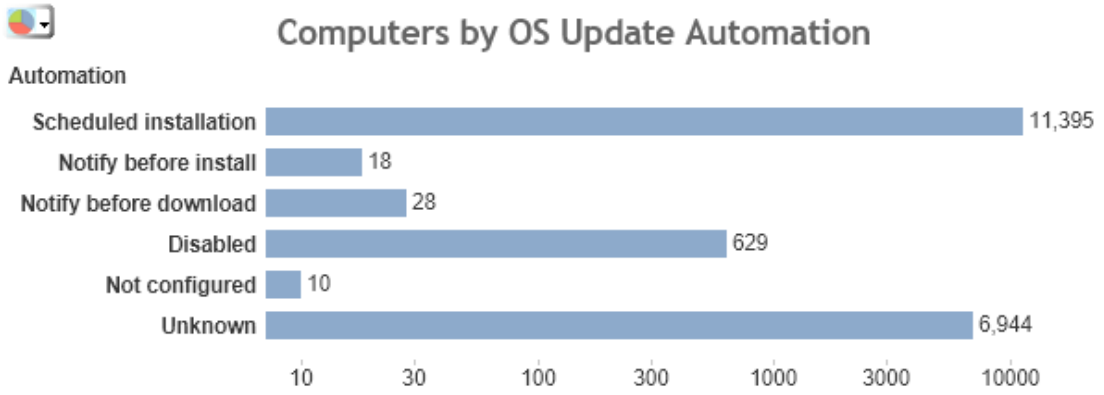
Sample reports: Vulnerabilities



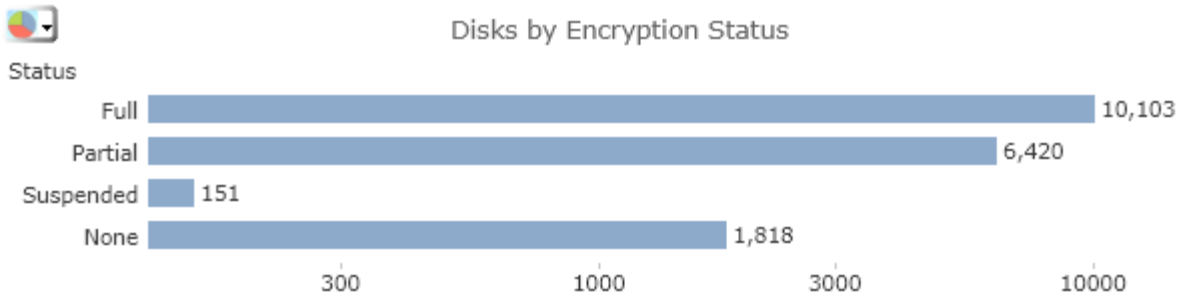
Vendor	Name	Bulletin Id	Severity	Installed	Missing
Adobe	APSB16-23	APSB16-23	Critical	0	13
Adobe	APSB20-23	APSB20-23	Critical	0	7
Adobe	APSB21-31	APSB21-31	Critical	0	12
Adobe	APSB22-52	APSB22-52	Critical	0	2
Adobe	APSB23-01	APSB23-01	Critical	0	382
Adobe	APSB23-11	APSB23-11	Critical	0	15
Adobe	APSB23-21	APSB23-21	Critical	0	267
Adobe	APSB23-23	APSB23-23	Critical	0	220
Adobe	EOL-Adobe	EOL-ADOBE	EOL	0	396
Apple	EOL-Apple	EOL-APPLE	EOL	0	194
Apple	HT206091	HT206091	Critical	0	115
Apple	HT213259	HT213259	Critical	0	222
Apple	HT213538	HT213538	Critical	0	2

Update provider and automation

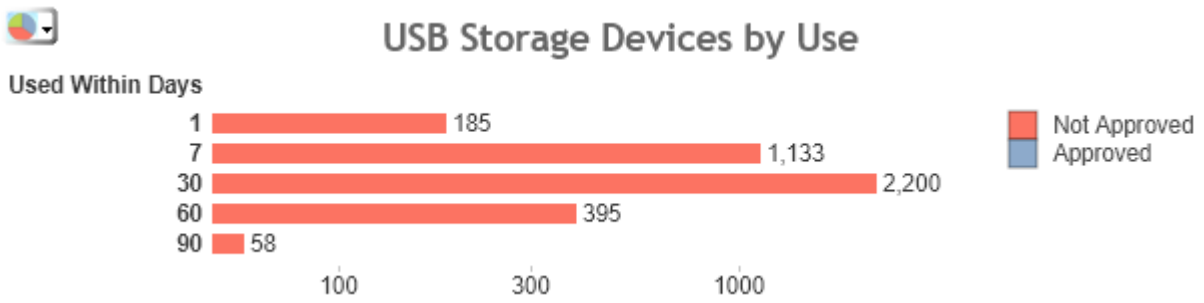




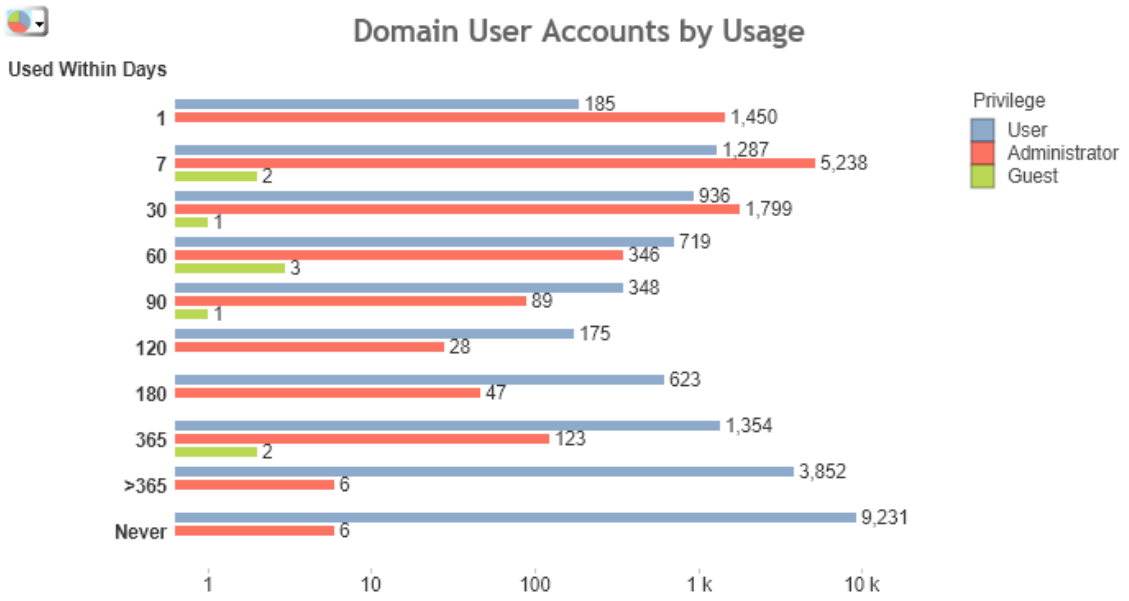
Disk encryption status

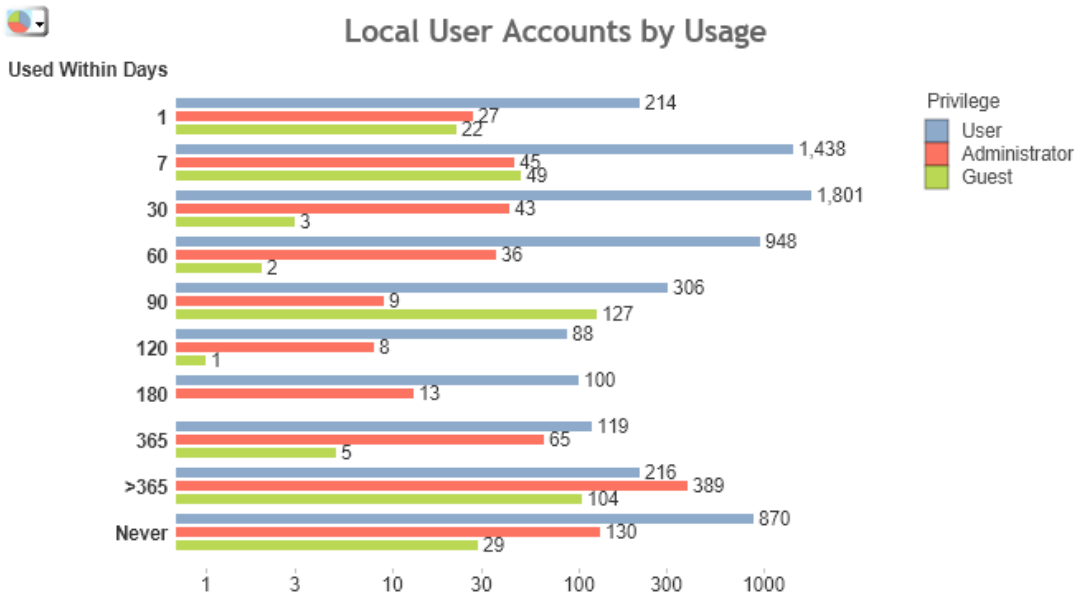


USB Storage Device Usage

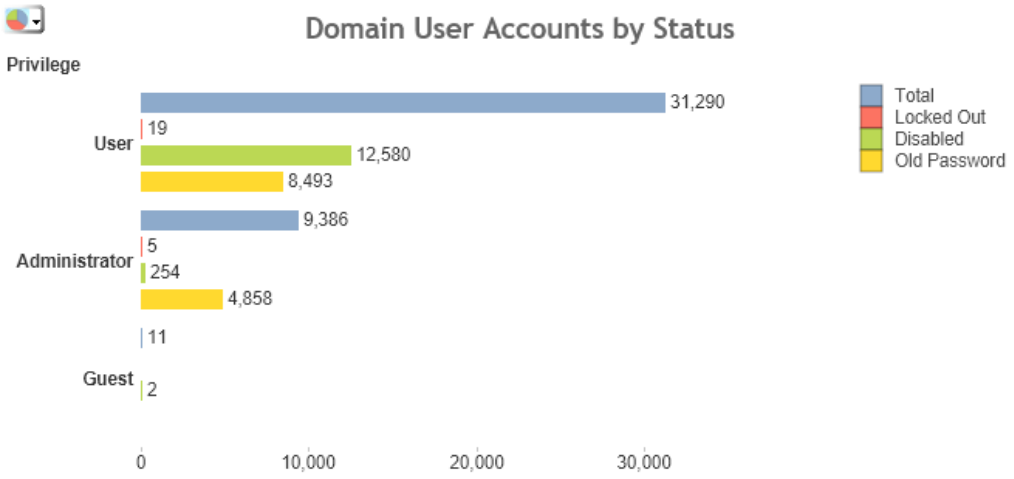


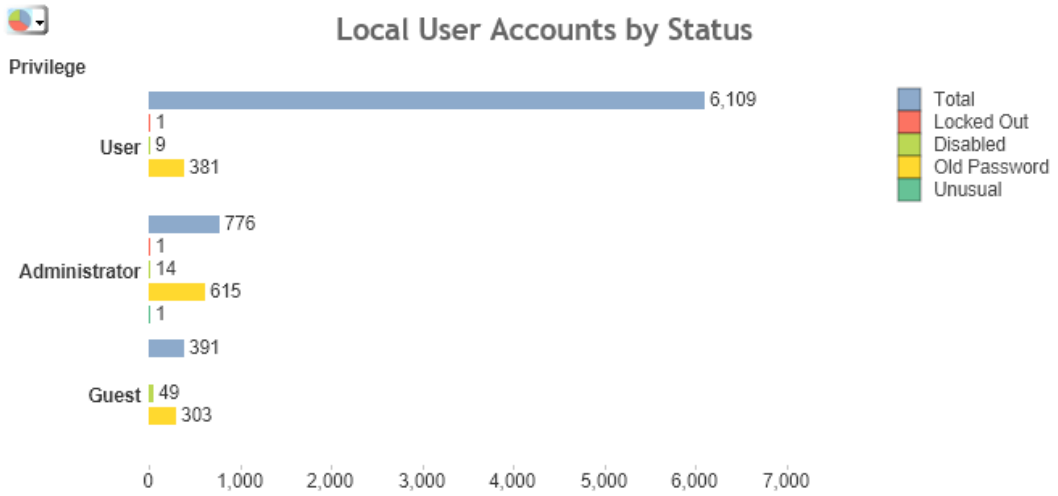
Domain & Local User Account Privileges





Domain & Local Account Status





Recommendations

- SAM should be a Data Provider, not just a Data Requestor
  - Detailed and normalized software, hardware, security data.
  - Detailed and normalized purchase data.
- SAM should share this data with others in the organization
  - Cybersecurity, Vendor Management, Operations, Finance, HR, Business Units
  - Data needs to be accurate, complete and up-to-date
    - If not, its useless, i.e. like many CMDB projects.

BELARC

About Belarc

- Over 1,800 customers worldwide
  - Commercial
    - Autodesk, GE Steam Power (France), Novelis (Canada, Korea), Shell Canada, Travelers Insurance (India)
  - US Federal Government
    - Bureau of Land Management, 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 over 40 countries
- Eight US and Worldwide Patents
  - Software usage.

Questions?

Sumin Tchen

Belarc, Inc.

stchen@belarc.com

www.Belarc.com