Vulnerability Management and Policy Compliance Dashboards

ZW Owned by Zshaquel Walker •••

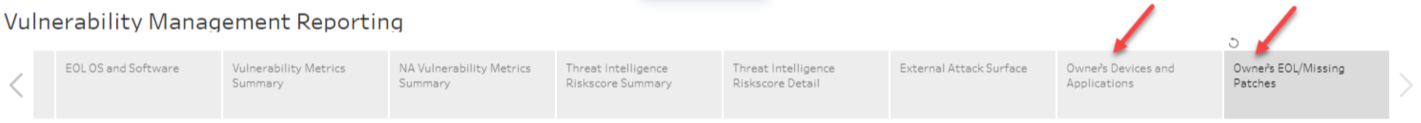
Last updated: Jun 25, 2024 • 5 min read • 2 people viewed • Attachments

Technical device and application owners can access [redacted] reports, specific to the hardware and software they own and manage within their groups (network, infrastructure, Digital, etc.), to review outstanding tasks related to unpatched or end-of-life software, OS and components, exploitable vulnerabilities detected, open risks and policy compliance. The following guide will assist users in navigating through the Owner's View dashboards. The owners are expected to leverage these views displaying enriched data, to manage their vulnerabilities/risks and policy compliance action items, at least quarterly as per [redacted] Information Security and Protection. Feel free to reach out to infrastructure team for vulnerability management or policy compliance. You can also reach out to the security team.

[redacted]

To begin, please visit General - I[redacted] Vulnerability Views>Vulnerability Management Reporting and use the scroll bar at the top, to locate the Owner's Devices and Applications and Owner's EOL/Missing Patches dashboards.

Comment

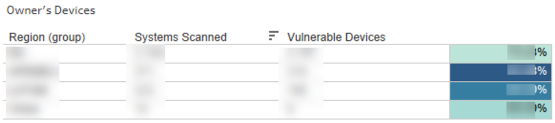


Vulnerability Management Reporting

EOL OS and Software
Vulnerability Metrics Summary
NA Vulnerability Metrics Summary
Threat Intelligence Riskscore Summary
Threat Intelligence Riskscore Detail
External Attack Surface
Owner's Devices and Applications
Owner's EOL/Missing Patches

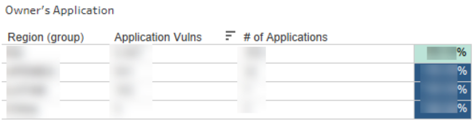
The Owner's Devices and Applications dashboards details:

- The # of devices scanned by [redacted] agents and the # of devices vulnerable, by region
  - EX: 2,754 systems scanned/2,055 vulnerable = 74.62% of devices are vulnerable
- The # of vulnerabilities detected on applications and the # if applications associated with vulnerabilities
  - EX: 358 represents number of applications. 3,380 total number of application vulnerabilities = 86.59% total vulnerable applications, so about 307.
- Risks specific to vulnerabilities, exceeding 90 days and not remediated through patching process or EOL assets pending decommission or EOL software requiring version update or product replacement
- The full list of vulnerable devices and applications, the impacted host/s and IP/s, along with the [redacted] description and # of vulnerabilities, categorized by the assigned owners
  - Suggest sorting by application [redacted]



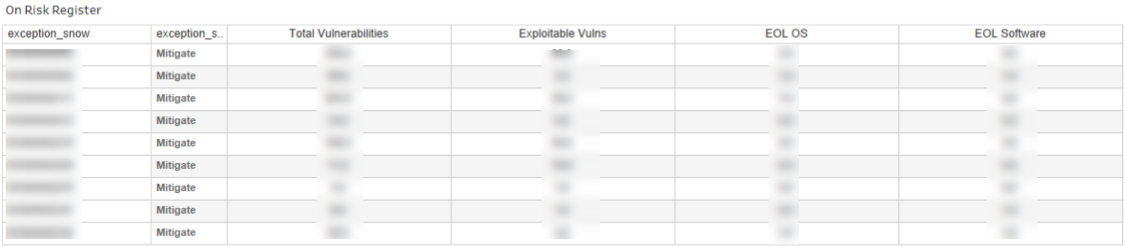
Owner's Devices

Region (group)	Systems Scanned	Vulnerable Devices	
[redacted]	[redacted]	[redacted]	[redacted]%
[redacted]	[redacted]	[redacted]	[redacted]%
[redacted]	[redacted]	[redacted]	[redacted]%
[redacted]	[redacted]	[redacted]	[redacted]%



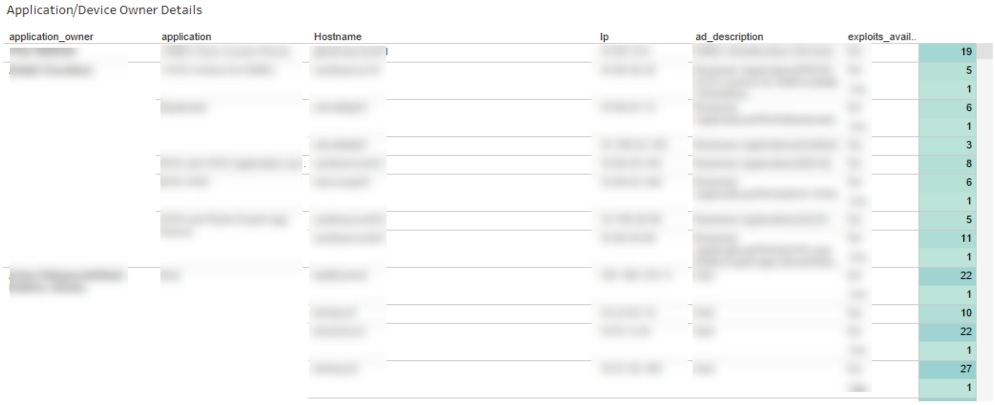
Owner's Application

Region (group)	Application Vulns	# of Applications	
[redacted]	[redacted]	[redacted]	[redacted]%
[redacted]	[redacted]	[redacted]	[redacted]%
[redacted]	[redacted]	[redacted]	[redacted]%
[redacted]	[redacted]	[redacted]	[redacted]%



On Risk Register

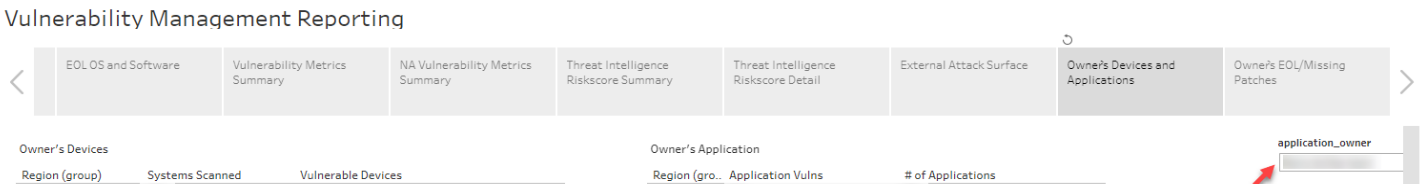
exception_snow	exception_s..	Total Vulnerabilities	Exploitable Vulns	EOL OS	EOL Software
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Mitigate	[redacted]	[redacted]	[redacted]	[redacted]



Application/Device Owner Details

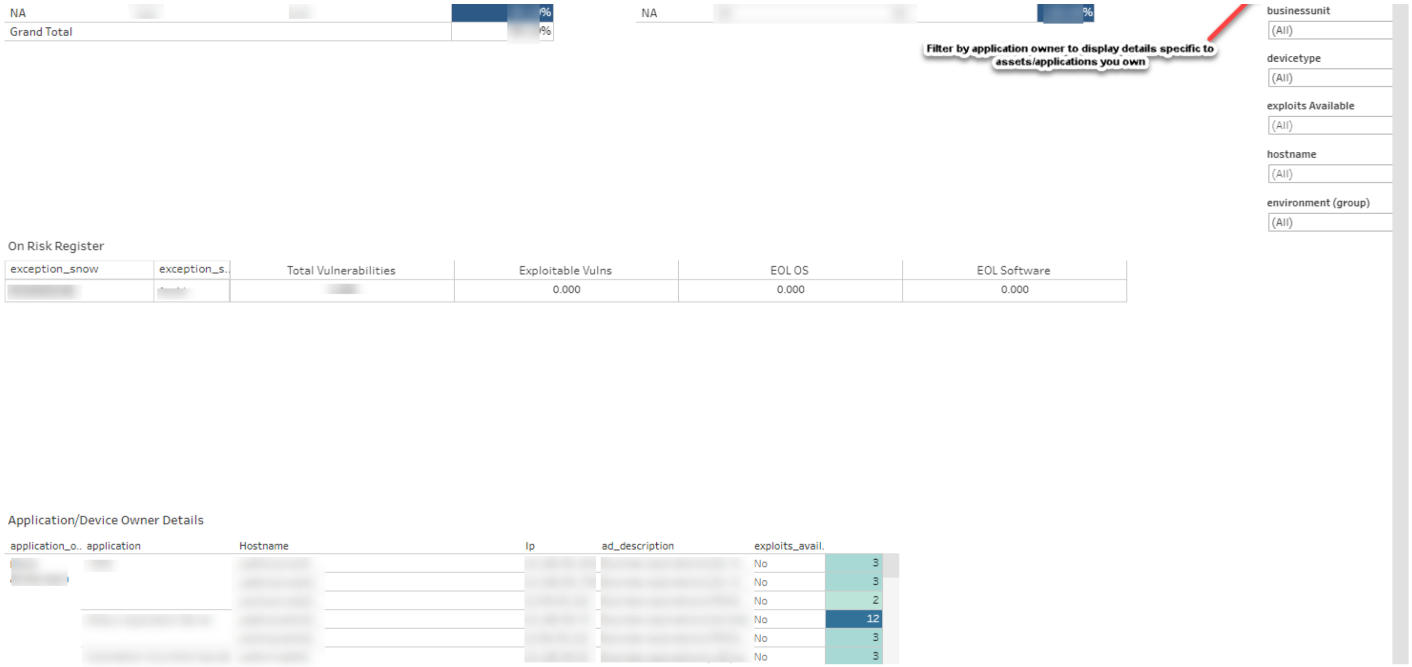
application_owner	application	Hostname	Ip	ad_description	exploits_avail..	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	19
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	5
					[redacted]	1
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	6
					[redacted]	1
		[redacted]	[redacted]	[redacted]	[redacted]	3
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	8
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	6
					[redacted]	1
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	5
		[redacted]	[redacted]	[redacted]	[redacted]	11
					[redacted]	1
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	22
					[redacted]	1
		[redacted]	[redacted]	[redacted]	[redacted]	10
		[redacted]	[redacted]	[redacted]	[redacted]	22
					[redacted]	1
		[redacted]	[redacted]	[redacted]	[redacted]	27
					[redacted]	1

Filters located on the right, allow owners to sort all reports within the dashboard, to specific details they'd wish to view, application/device owner, business unit, device type, exploitable vulnerabilities and environment.



Vulnerability Management Reporting

EOL OS and Software
Vulnerability Metrics Summary
NA Vulnerability Metrics Summary
Threat Intelligence Riskscore Summary
Threat Intelligence Riskscore Detail
External Attack Surface
Owner's Devices and Applications
Owner's EOL/Missing Patches
Owner's Devices
Region (group)
Systems Scanned
Vulnerable Devices
Owner's Application
Region (gro..
Application Vulns
# of Applications
application_owner



NA	[redacted]	[redacted]	[redacted]%
Grand Total			[redacted]%

NA	[redacted]	[redacted]%

Filter by application owner to display details specific to assets/applications you own

businessunit
(All)
devicetype
(All)
exploits Available
(All)
hostname
(All)
environment (group)
(All)

On Risk Register

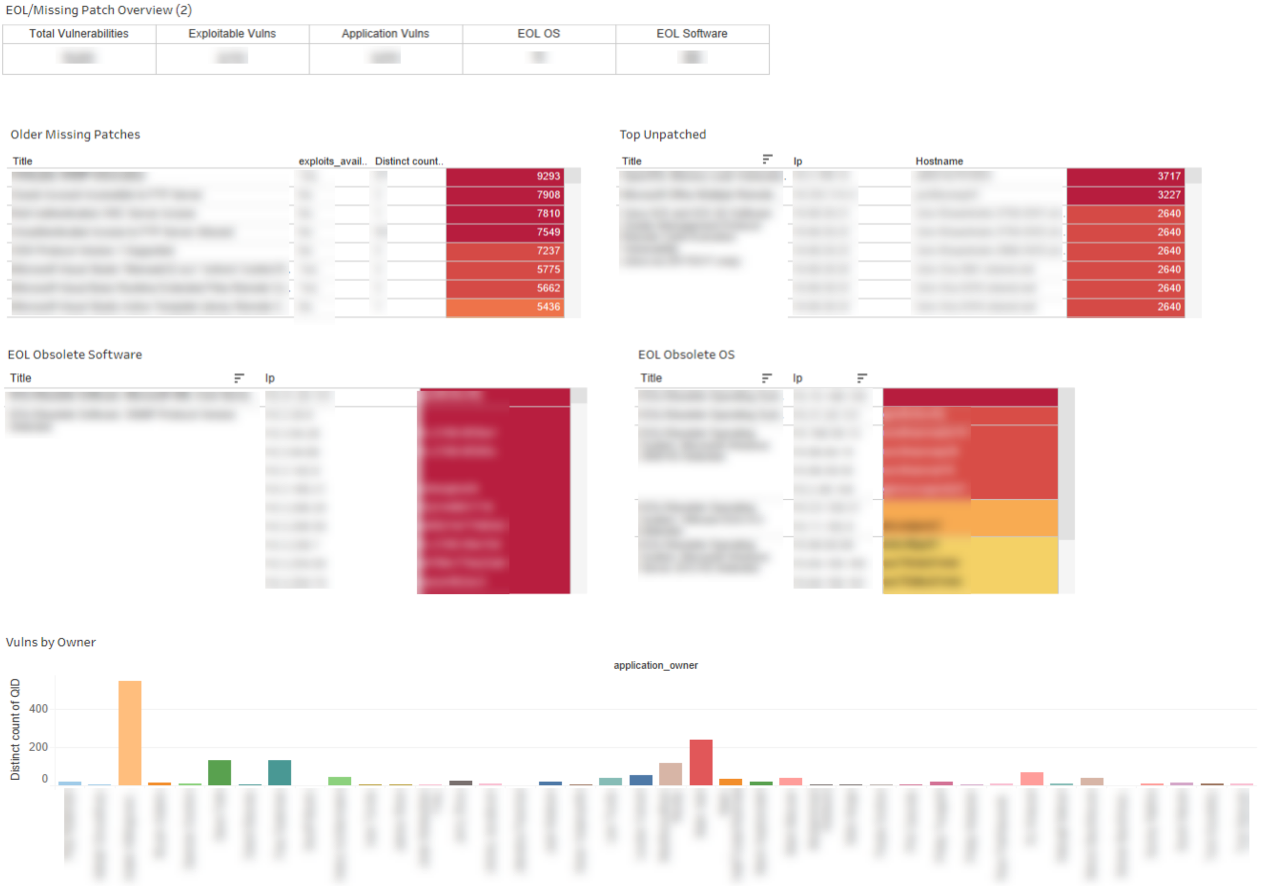
exception_snow	exception_s..	Total Vulnerabilities	Exploitable Vulns	EOL OS	EOL Software
[redacted]	[redacted]	[redacted]	0.000	0.000	0.000

Application/Device Owner Details

application_o..	application	Hostname	Ip	ad_description	exploits_avail.	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	No	3
		[redacted]	[redacted]	[redacted]	No	3
		[redacted]	[redacted]	[redacted]	No	2
	[redacted]	[redacted]	[redacted]	[redacted]	No	12
		[redacted]	[redacted]	[redacted]	No	3
	[redacted]	[redacted]	[redacted]	[redacted]	No	3

The Owner's EOL/Missing Patches dashboard details:

- An overview of the total # of vulnerabilities, exploitable vulnerabilities, application vulnerabilities, end-of-life operating systems and end-of-life software
- Systems and applications unpatched longer than 90 days or one full patching cycle
- Systems and applications unpatched longer than 90 days or one full patching cycle, with critical and high risk scores detected in [redacted] and [redacted] and exploits available
- End-of-life software
- End-of-life systems
- A grid to display # of vulnerabilities and the owners assigned to remediation



EOL/Missing Patch Overview (2)

Total Vulnerabilities	Exploitable Vulns	Application Vulns	EOL OS	EOL Software
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Older Missing Patches

Title	exploits_avail..	Distinct count..
[redacted]	[redacted]	9293
[redacted]	[redacted]	7908
[redacted]	[redacted]	7810
[redacted]	[redacted]	7549
[redacted]	[redacted]	7237
[redacted]	[redacted]	5775
[redacted]	[redacted]	5662
[redacted]	[redacted]	5436

Top Unpatched

Title	Ip	Hostname	
[redacted]	[redacted]	[redacted]	3717
[redacted]	[redacted]	[redacted]	3227
[redacted]	[redacted]	[redacted]	2640
	[redacted]	[redacted]	2640
	[redacted]	[redacted]	2640
	[redacted]	[redacted]	2640
	[redacted]	[redacted]	2640
	[redacted]	[redacted]	2640

EOL Obsolete Software

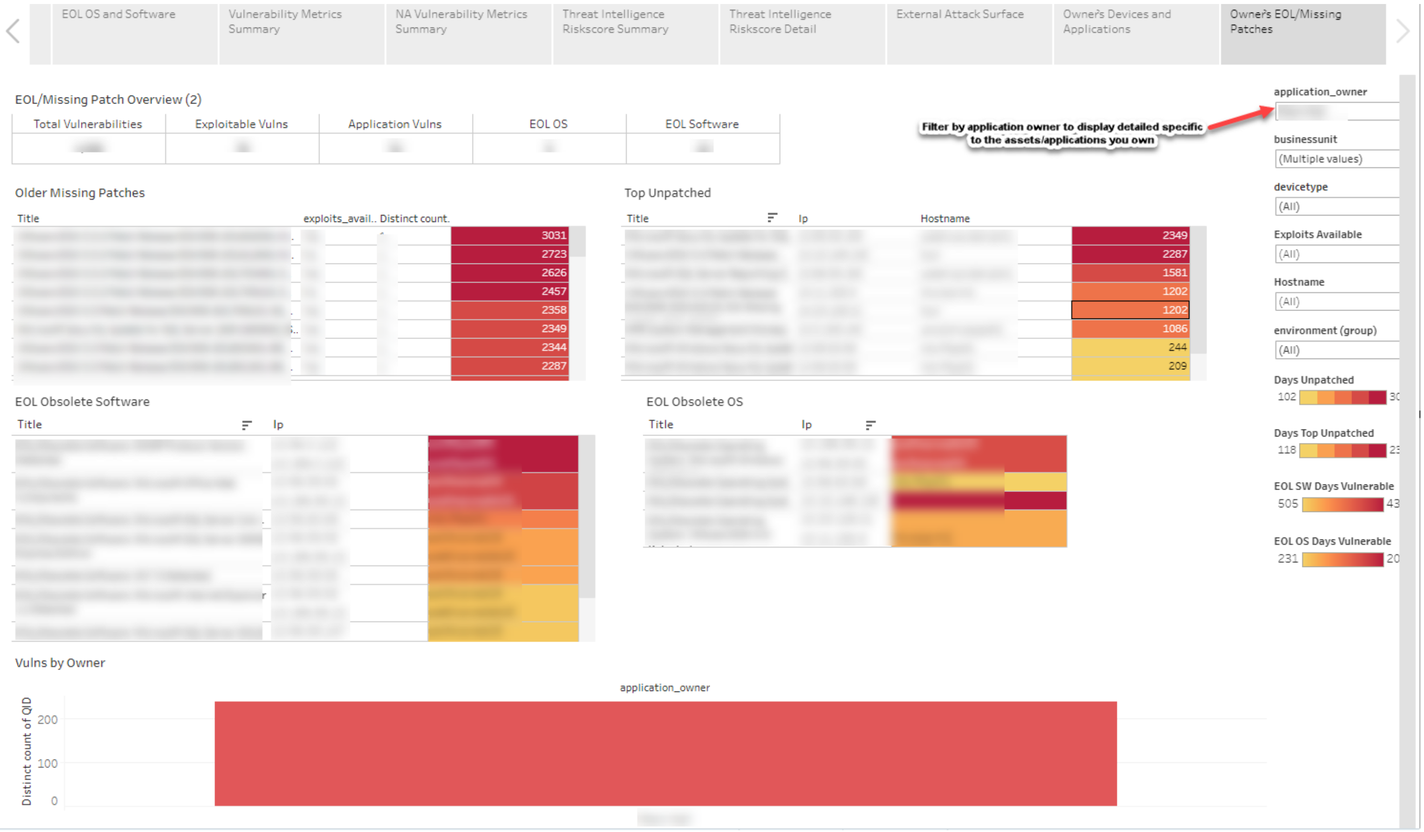
Title	Ip	
[redacted]	[redacted]	[redacted]

EOL Obsolete OS

Title	Ip	
[redacted]	[redacted]	[redacted]

Vulns by Owner

Filters located on the right, allow owners to sort all reports within the dashboard, to specific details they'd wish to view, application/device owner, business unit, device type, exploitable vulnerabilities and environment.



Filter by application owner to display detailed specific to the assets/applications you own

Policy compliance metrics are based on CIS benchmarks, best practices, service control polices, etc. Owners are expected to review for policy controls that are failing and follow up with the appropriate team to determine if controls need to be applied, and if these is a specific reason a control cannot be implemented, an exception request should be escalated and registered within the risk register.

Domain controllers, windows/GPO - Security team [redacted]

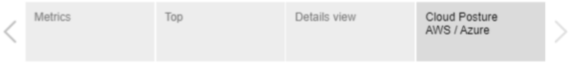
Cloud infrastructure team - [redacted]

Network - [redacted]

Infrastructure team - [redacted]

To review dashboard specific to policy compliance, please visit General - [redacted] use the scroll bar at the top, to locate the desired dashboard.

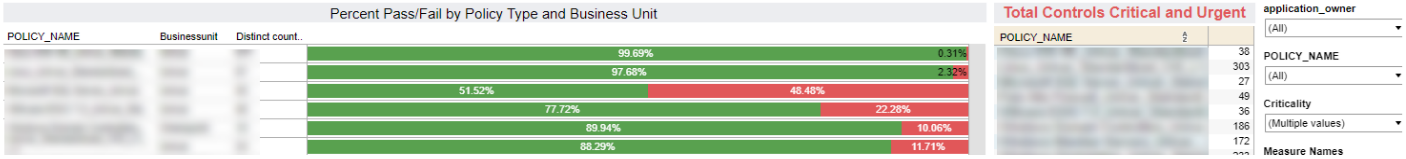
Policy Compliance View

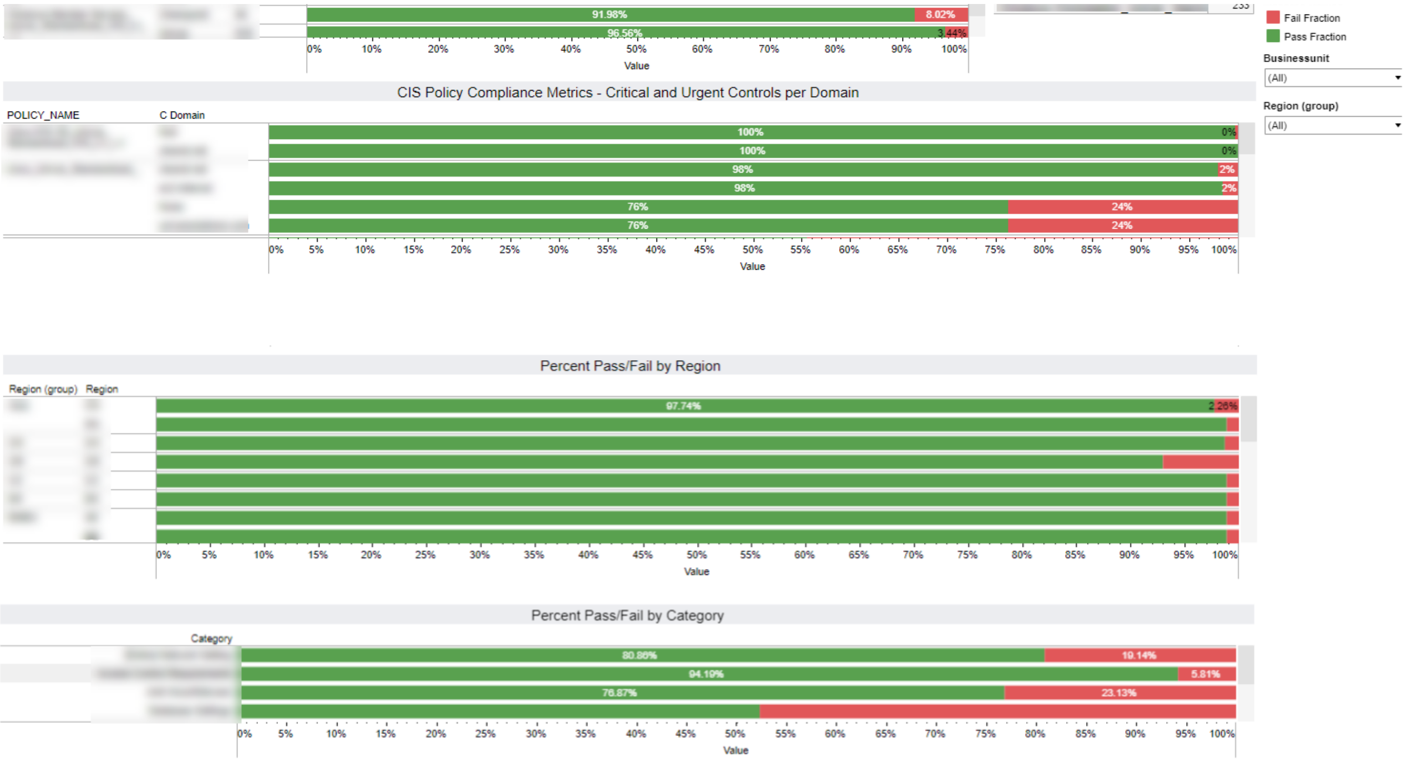


The Metrics dashboard details:

- Percent Pass/Fail by Policy Type and Business Unit
  - Percent failing represents the number of distinct controls that are failing
- Total Controls Critical and Urgent
  - most important policies/benchmarks and the Distinct count of Control ID is the number of failing controls under the specific policy
    - CIS benchmarks are configuration baselines and best practices for securely configuring a system.
    - Each of the guidance recommendations references one or more CIS controls that were developed to help organizations improve their cyberdefense capabilities.
      - acceptable use policy - rules around accessing restricted information; changing access data, such as passwords; opening questionable email attachments; using public Wi-Fi services; and using company approved authentication procedures.
- CIS Policy Compliance Metrics - Critical and Urgent Controls per Domain
- Percent Pass/Fail by Region
- Percent Pass/Fail by Category

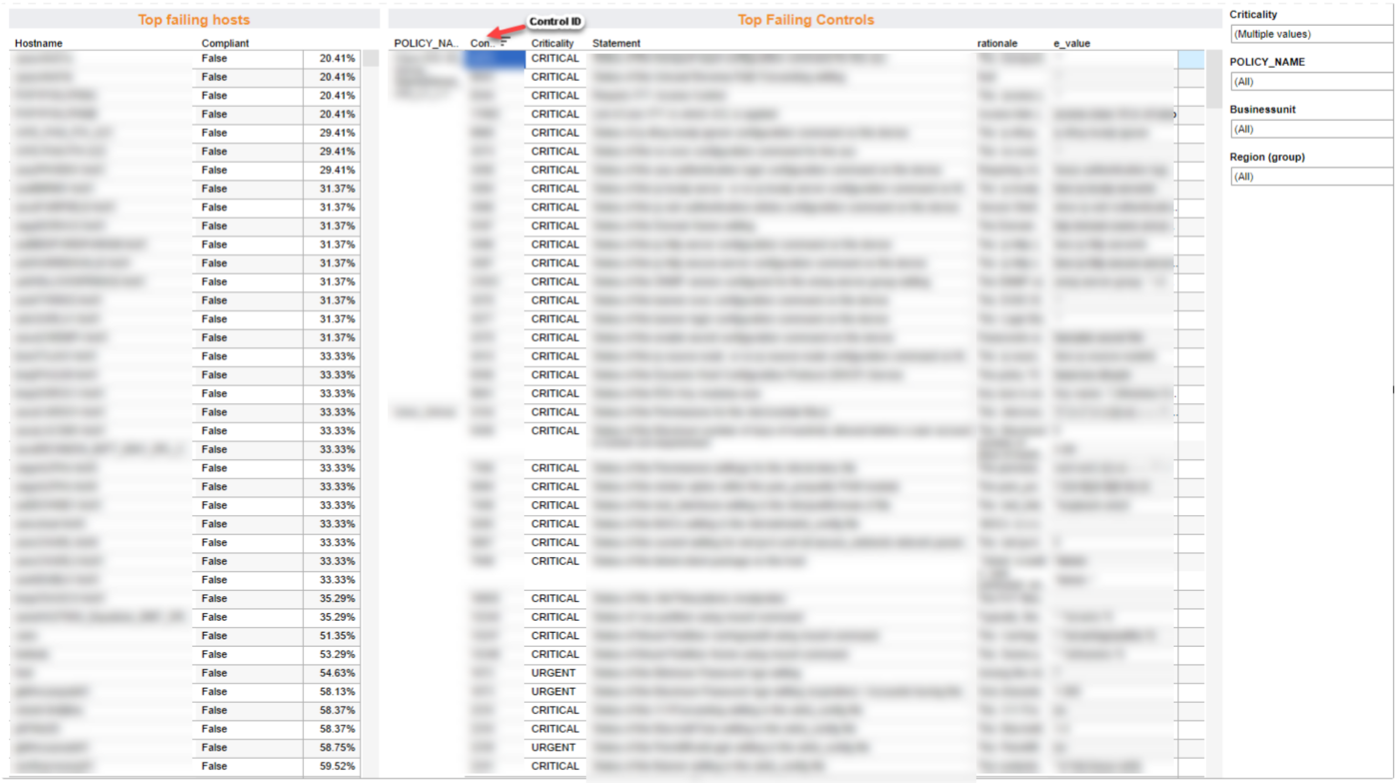
Filters located on the right, allow owners to sort all reports within the dashboard, to specific details they'd wish to view, application/device owner, criticality, policy name, business unit and region.





The Top dashboard details:

- Top failing hosts
- Top Failing Controls



Top failing hosts

Hostname	Compliant	
[redacted]	False	20.41%
[redacted]	False	20.41%
[redacted]	False	20.41%
[redacted]	False	20.41%
[redacted]	False	29.41%
[redacted]	False	29.41%
[redacted]	False	29.41%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	31.37%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	33.33%
[redacted]	False	35.29%
[redacted]	False	35.29%
[redacted]	False	51.35%
[redacted]	False	53.29%
[redacted]	False	54.63%
[redacted]	False	58.13%
[redacted]	False	58.37%
[redacted]	False	58.37%
[redacted]	False	58.75%
[redacted]	False	59.52%

Top Failing Controls

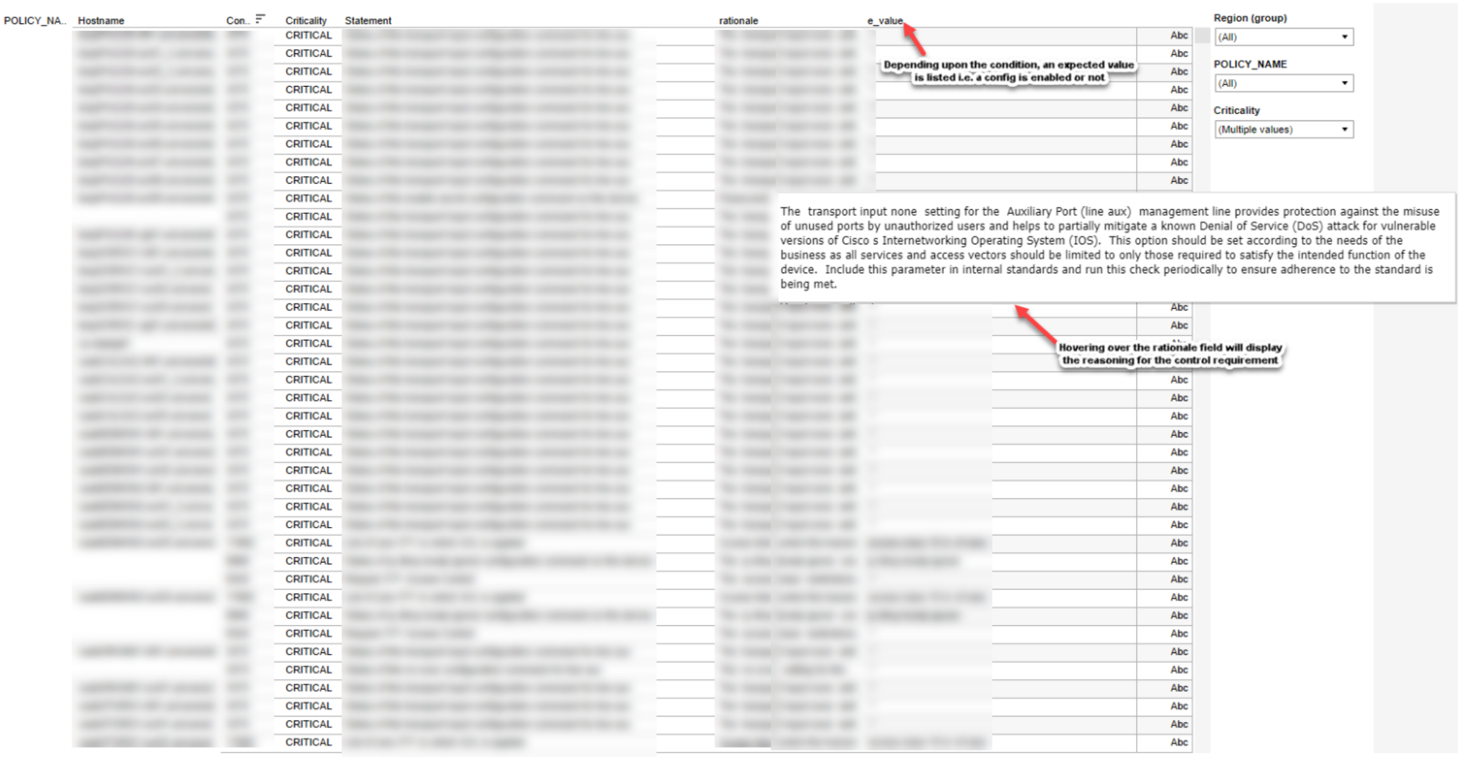
POLICY_NA..	Con..	Criticality	Statement	rationale	e_value
[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	URGENT	[redacted]	[redacted]	[redacted]
	[redacted]	URGENT	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]
	[redacted]	URGENT	[redacted]	[redacted]	[redacted]
	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]

The Details View dashboard reflects:

- Policy name
- Hostname associated with the policy
- Control ID
- Status of criticality
- Statement about the control in place
- Rationale as to why the control is in place

- Expected value

Filters located on the right, allow owners to sort the report by Region, Policy Name or Criticality.



POLICY_NA..	Hostname	Con..	Criticality	Statement	rationale	e_value	
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		
		[redacted]	CRITICAL	[redacted]	[redacted]		
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]		
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
		[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
		[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
		[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
		[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
		[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc
	[redacted]	[redacted]	CRITICAL	[redacted]	[redacted]	[redacted]	Abc

Region (group): (All)

POLICY_NAME: (All)

Criticality: (Multiple values)

Depending upon the condition, an expected value is listed i.e. a config is enabled or not

The transport input none setting for the Auxiliary Port (line aux) management line provides protection against the misuse of unused ports by unauthorized users and helps to partially mitigate a known Denial of Service (DoS) attack for vulnerable versions of Cisco s Internetworking Operating System (IOS). This option should be set according to the needs of the business as all services and access vectors should be limited to only those required to satisfy the intended function of the device. Include this parameter in internal standards and run this check periodically to ensure adherence to the standard is being met.

Hovering over the rationale field will display the reasoning for the control requirement

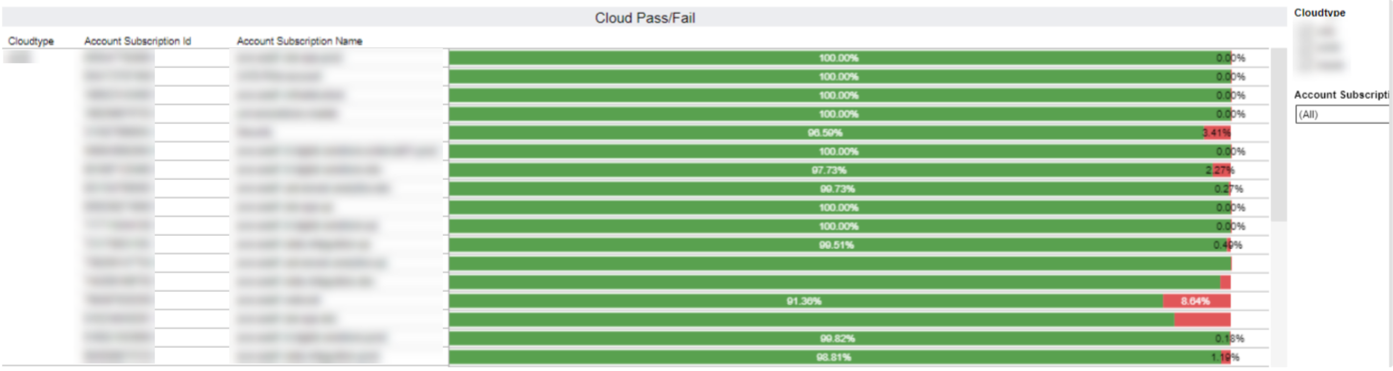
The [redacted] dashboard details:

Cloud Pass/Fail - percentage of assets (virtual machine, database, storage bucket, etc.), with passing or possible failing controls

Cloud Top Control - most critical controls

Cloud Top Account - most critical accounts

Filters located on the right, allow owners to sort the report by Cloud Type and Account Subscription

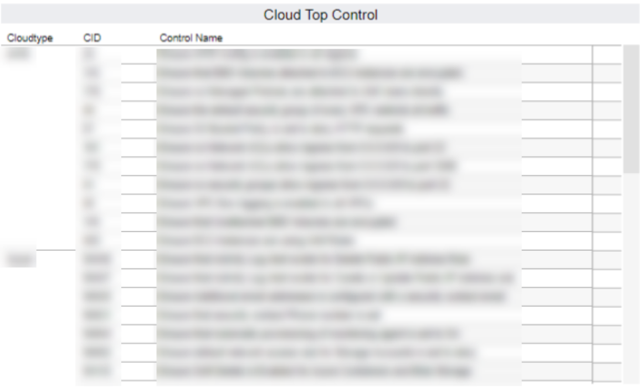


Cloud Pass/Fail

Cloudtype	Account Subscription Id	Account Subscription Name	Pass	Fail
[redacted]	[redacted]	[redacted]	100.00%	0.00%
	[redacted]	[redacted]	100.00%	0.00%
	[redacted]	[redacted]	100.00%	0.00%
	[redacted]	[redacted]	100.00%	0.00%
	[redacted]	[redacted]	96.59%	3.41%
	[redacted]	[redacted]	100.00%	0.00%
	[redacted]	[redacted]	97.73%	2.27%
	[redacted]	[redacted]	99.73%	0.27%
	[redacted]	[redacted]	100.00%	0.00%
	[redacted]	[redacted]	100.00%	0.00%
	[redacted]	[redacted]	99.51%	0.49%
	[redacted]	[redacted]		
	[redacted]	[redacted]		
	[redacted]	[redacted]	91.36%	8.64%
	[redacted]	[redacted]		
	[redacted]	[redacted]	99.82%	0.18%
	[redacted]	[redacted]	98.81%	1.19%

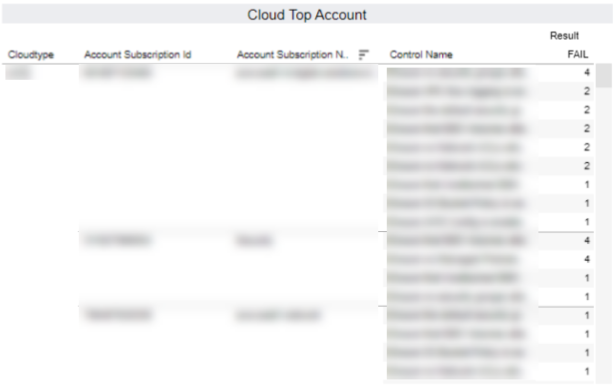
Cloudtype: [redacted]

Account Subscripti: (All)



Cloud Top Control

Cloudtype	CID	Control Name
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]



Cloud Top Account

				Result
Cloudtype	Account Subscription Id	Account Subscription N..	Control Name	FAIL
[redacted]	[redacted]	[redacted]	[redacted]	4
			[redacted]	2
			[redacted]	2
			[redacted]	2
			[redacted]	2
			[redacted]	2
			[redacted]	1
			[redacted]	1
			[redacted]	1
	[redacted]	[redacted]	[redacted]	4
			[redacted]	4
			[redacted]	1
			[redacted]	1
	[redacted]	[redacted]	[redacted]	1
			[redacted]	1
			[redacted]	1
			[redacted]	1

+ Add label

Related pages ⓘ

Tableau Dashboards
[redacted]
More like this

Tableau Report Subscription
IT Compliance
Organized together

Agiloft Dashboard
[redacted]
More like this

Measuring Risk
IT Compliance
Organized together

WIMS Dashboard
[redacted]
More like this

IT Security Assessment Process
IT Compliance
Organized together

👍 👏 🎉 ☺ Be the first to add a reaction

ZW Write a comment...