### THE BEDROCK OF CYBER SECURITY



Solutions Architect / Axonius







What is SOCI and Why?

**Security Process Improvement** 

Maintaining Compliance

**Security Process Automation** 

**Questions?** 



# What is SOCI?

**3** Object

The object of this Act is to provide a framework for managing risks relating to critical infrastructure, including by:

(a) improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and

(b) facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks; and

(c) requiring responsible entities for critical infrastructure assets to identify and manage risks relating to those assets; and
(d) imposing enhanced cyber security obligations on relevant entities for systems of national significance in order to improve their preparedness for, and ability to respond to, cyber security incidents; and
(e) providing a regime for the Commonwealth to respond to

(e) providing a regime for the Commonwealth to respond to serious cyber security incidents.



#### **Security Process Compliance**

## Change of current process

### Business Process Improvement



#### **Security Process Compliance**

# SOCI is only ONE driver for Business Security Process Improvement



- 1. Assess your current state
- 2. Define your future State
- 3. Define performance metrics
- 4. Identify and prioritise improvement
- 5. Create a process improvement plan



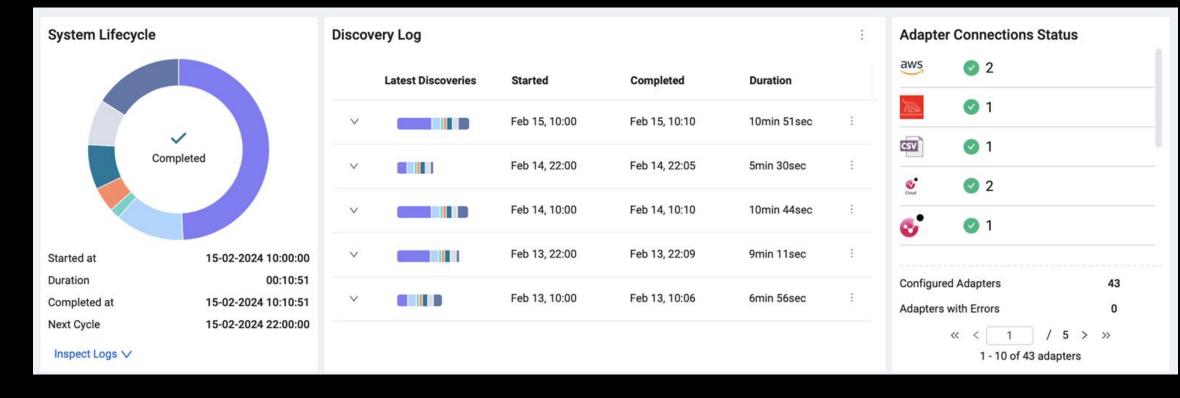
- Manual Audit
- Interview stakeholders
- Review individual processes
- Data Mining Capability

Integration with all existing tools

Extract and aggregate Asset Data continuously

Allows analysis of the Holistic Current and Historical State of Assets





Dev	ice Discovery		:	User Discovery		:
0	ServiceNow	4,323 (4,491)		() Tenable.io	1,608	
	McAfee ePolicy Orchestrator (ePO)	3,630		ServiceNow	1,608	
	Palo Alto Networks Panorama	3,163		C Zoom	1,602	
diada esco Meraki	Cisco Meraki	2,645		Slack	1,602	
¢	Tanium Client Status	2,253		G Google Workspace (G Suite)	1,602	
	Tanium Asset	2,253		Okta	1,569	
<)	ForeScout CounterACT	2,198		Microsoft Azure Active Directory (Azure AD) and Microsoft Intune	817 (1,060)	
G	Google Workspace (G Suite)	1,870		Salesforce	473 (489)	
CC.	Claroty	1,850		Have I Been Pwned	362 (369)	
	Zoom	1,439		Microsoft Active Directory (AD)	243	
٢	Tenable.io	1,110 (1,136)		Bloodhound	15	
٢	Tenable.sc (SecurityCenter)	1,004 (1,044)		Zscaler Web Security	13 (14)	
0	Trend Micro Deep Security	991		Amazon Web Services (AWS)	6	
8	CylancePROTECT	967				
٢	Check Point CloudGuard	963				
Axonius	evices seen s Devices Correlation nique Devices		41569 (41803) <b>T</b> 5376	Total Users seen Axonius Users Correlation Total unique Users		20 (11787) <b>T</b> 1608

04

Users															Asset Investigation >		Sav	ed Qu	eries >
New Query	Save As	Reset	EC Actions 🗸	Dis	splay by Dat	e													
Q ("adap	ters_data.active_director	y_adapter.is_ad	min" == true) ar	nd ("adapte	ers_data.okt	a_adap	oter.is_a	idmin" =:	= true)							,		Quer	y Wizard
Total 4					Show Us	ers											Refin	e all Fi	ields   ~
					WHERE	- (	NOT	ALL -	-	•	Is Admin	•	yes	-	)	<b>I</b> ₽		P	⊚ ×
	Adapter Connections		ß	User Na	AND	- (	NOT	ALL -	- 0	) -	Is Admin	*	yes	-	)	<b>⊡</b>		P	⊚×
	📑 🚸 G 🔚 O	🗢 🔿 🌵	10 🖸	robin.rol						0								_	
	📢 🚸 Ġ 📴 O	🗢 🔿 👬	💿 🧿	young.w	+														
	📢 🚸 G o 🐡	0 👬 🚳	•	william.v											c	lear		Sea	arch
	📢 🗇 🖸 O 🔿	i 🎼 🚳 🔾		charles.es	sier@demo.	ocal		demo	local		Yes No	0		15-02-2024	4 09:37:21 admin	Suite	User	Needs	SSO

Devices												Asset Investigat	ion >		Save	ed Que	eries
New Query Sav	ve As Reset	EC Action	ns v 🛛 [	Display by D	ate												
Q (("adapters_data	a.aws_adapter.public_ip	s" == ({"\$exists":	true,"\$ne":[]})))	and ("adapt	ers_data.	aws_ada	apter.firev	vall_rules.d	irection" == "INGRESS") an	l not ("adapters_	data.tenab	le_io_adapter.last	_scann	ed" ; <del>▼</del>		Query	y Wiza
Total 165				Show I	Devices											_	
Adapter	Connections		E		Compose	query ir	n regular E	English							×		▶ Go
🗆 🗸 aws 🦿	cisco. 🕬 🚺	🔍 🛛 🖉 🤇													Refine	e all Fi	ields
	isco. 🔍 👿 🗴	🖉 🕪 🔿 🍯	<b>  C</b> 💿 (	WHER	E 👻 (	NOT	ALL 👻	aws -	Public IPs	🕶 exists 👻	]		)	∎		70	0
🗆 🗸 aws 🦿	CISCO. CAROTY	🤹 👿 🜌 🕷	0 🔽 🤇	AND	-	NOT	ALL 👻	aws 👻	Firewall Rules: Direction	✓ equals	INGRESS	6	• )	∎		\$	$\odot$
🗌 🗸 aws 🦿	🧯 🚓 🔬 💓 🔇	🖉 🔘 🍯	<b>G</b> 💿 💿	AND	<b>-</b> (	NOT	ALL 👻	(io) –	Last Scanned	🕶 last da 👻	14		)	I.		æ	0
aws a	👯 🥴 🚺 🕅	🗰 🔘 🎽	<b>G</b> 💿 💿	AND		NOT	ALL 👻	<b>•</b>	ID	🕶 exists 👻	]		)	IP	0ì	7⊕	$\odot$
aws a	🔬 🔮 👿 🖉 🜌	• • •	o 💿										,				0
🗆 🗸 aws 🦿	cisco. 🔊 🖤	8 🖉 🔘 🧲	, 🖸 🐠	+													
	isco. 💔 🙎 👿 🖣	3 🖪 🔿 🖨	💿 💿										(	Clear		Sea	arch
aws u	ulu 🚓 以 👿	8 🛯 🔿 🗲	, 💿 🝈	aws	s-webngir	าx-4265เ	)97-prod.(	demo.loca	Linux Red Ha	8		14	-02-202	24 1 5:5	3:30		10



**Guidance of future state is prescribed by SOCI** 

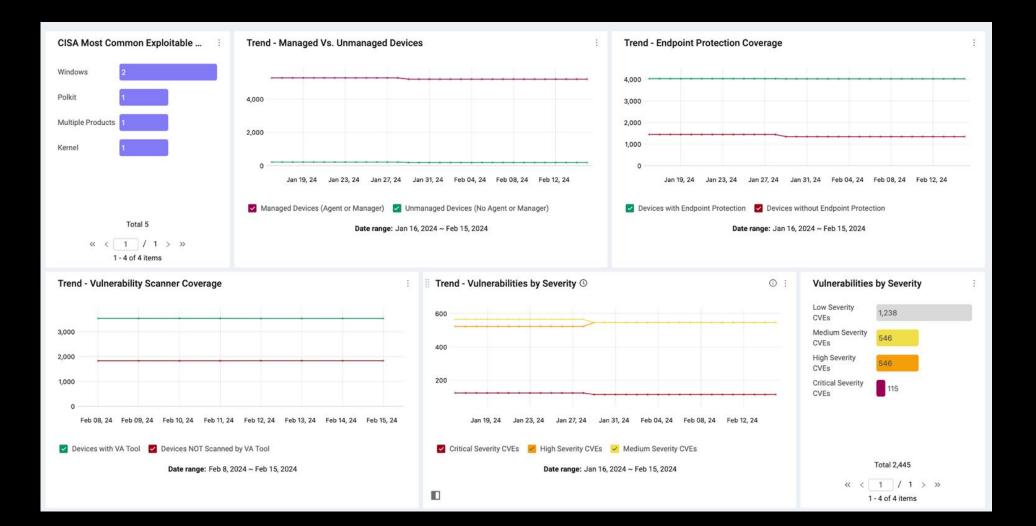
With Asset Intelligence the Delta between current state and the future compliant state can be objectively measured



Asset Intelligence assists by *Indicating what is currently possible* and allowing *further analysis* of Assets data to validate proposed metrics.

#### Asset Intelligence facilitates moving to a state of continuous compliance.







# Asset Intelligence provides the context required to confidently automate processes.



ServiceNow - Create Incident Demisto - Create Incident per Asset	Opsgenie - Create Alert Jira Service Management - Create Issue per Asset	Adobe Workfront - Create Issue	ServiceNow - Create Incident per Asset	Create ticket for missing ePO on Windows          + Add description         * Run action on assets matching following query:         Image: Devices       V         Windows devices missing McAfee ePolicy Orchestrator (ePO) software         Main Action         Image: Optimized serviceNow - Create Incident (?)         * Action name
ServiceNow - Create Incident Cherwell - Create Incident Demisto - Create ChangeGear - Create	Alert	Adobe Workfront - Create Issue	ServiceNow - Create Incident per Asset	* Run action on assets matching following query:   Image: Devices V   Windows devices missing McAfee ePolicy Orchestrator (ePO) software   Main Action   C ServiceNow - Create Incident ③   Test Connection
Incident Incident Demisto - Create ChangeGear - Create	Alert	Create Issue	Incident per Asset	Image: Devices       V         Windows devices missing McAfee ePolicy Orchestrator (ePO) software         Main Action         Image: Operation of the second
Demisto - Create ChangeGear - Create	Management - Create		Freshservice Create	ServiceNow - Create Incident (?)
Demisto - Create ChangeGear - Create	Management - Create		Freshservice Create	
Demisto - Create Incident per Asset ChangeGear - Create Incident	Management - Create			* Action name
		Devops - Oreate Task		Ticket to Install McAfee ePO on Windows
			noket per Asset	
				Configure Dynamic Values ①
<b>9 0</b>	4	ZK	4	Use stored credentials from the ServiceNow adapter
Freshservice - Create Update ServiceNow Ticket Tickets	Jira Service Management - Update	Update Zendesk Tickets	Jira Service Management - Create	Select Adapter Connection ①
Holder Holdes	Tickets	Hoketa	Issue	65b69c50a3accae41a9dda1b
				*Incident short description
* 8	•>	A	>	McAfee ePO is required
SolarWinds - Create BMC Helix Remedy - Incident Create Ticket	Cherwell - Create Incident per Asset	SysAid - Create Incident	TOPdesk - Create Ticket	*Incident description
				These Windows devices do not have the required McAfee ePO agent installed. Route to the desktop team for remedia
				*Message severity
X X	adapters	)	)	error
Zendesk - Create Zendesk - Create Ticket Tickets Per Entity	Create Case - Salesforce	ManageEngine ServiceDesk Plus -	ManageEngine ServiceDesk Plus -	*Instance Name
There is any		Create Request	Create Request per A	Primary
2 8	TDX	Ω	P	Advanced options Save () Test Run Save and
Zoho Desk - Create Ticket BOSSDesk - Create Ticket	TeamDynamix - Create Ticket	CA Service Management - Create	Create Incident - PagerDuty	



By connecting to all the security and management solutions, Axonius helps customers:

- More accurately assess risk
- Track compliance maturity daily
- Respond rapidly to changing requirements and situations
- Facilitate Collaboration between teams for containment and remediation
- Optimise Processes and incorporate automation

Overview	Main Action: Image Qualys - Add IP Addresses as Host Assets Image Optimized Stress Add IP Addresses as Host Assets Image Optimized Stress Add Image Optim
* Enforcement Set name	* Action name
Add Windows Endpoints to Qualys configuration	Add IP's as Host Assets in Qualys
+ Add Description	Configure Dynamic Values ①
	*Qualys Cloud Platform domain
Run this Enforcement Set on assets matching the following query Q Active Windows Endpoints Not Seen by Qualys	qualys.internal
	*User name
Main Action	axonius
Qualys - Add IP Addresses as Host Assets	======================================
Success Actions	*rassword ************************************
	Additional Fields ∨
Syslog Server - Send Log Message	Additional Fields V
+	
Scheduling type O off	
() on	
	é
	ć
	ć
	<b>É</b>
	ć.
	ú.
	<pre></pre>



# **QUESTIONS?**

#### THANK YOU!



Solutions Architect / Axonius paul.thomas@axonius.com

