CYVATAR.AI

RACI

Solutions Role Navigator:

Defining Responsibilities for Seamless Cybersecurity Management

Table of Contents

Roles & Responsibilities

The Roles and Responsibilities are outlined for each of Cyvatar's Subscriptions using a simple roles and responsibilities matrix called a RACI Model. Below are the four roles used to assign the level of task responsibility:

R

Responsible
The person who is responsible for doing the work.

A

Accountable
The person who is ultimately accountable for the process or task being completed appropriately.

C

Consulted
People who are not directly involved with carrying out the task but whose opinions are sought.

I

Informed
Those who receive output from the process or task or have a need to stay in the know.

All Solutions

Task ownership is outlined below using the RACI Model.

Task:	Cyvatar	Member
Provide an internal point of contact for Cyvatar for activities including troubleshooting.	I	RAC
Provide relevant documentation, information on proposed applications and computing systems, users and data.	I	RAC
Responsible for network, host, and/or cloud availability at all times; lack of network, or cloud readiness may result in lack of productivity and ability for Cyvatar to provide services.	I	RAC
Provide access to appropriate individuals, as requested by Cyvatar.	I	RAC
Responsible for minimum bandwidth per host at all times; lack of network bandwidth may result in lack of productivity and ability for Cyvatar to provide services	I	RAC

Threat & Vulnerability Management (TVM)

Task ownership is outlined below using the RACI Model.

Task: Patch Management	Cyvatar	Member
Installation of patch management system	RCI	RA
Configuration of patch management system	RA	CI
Maintenance of patch management system	RA	CI
Change management	CI	RA
Issue review and resolution (to the extent reasonably possible)	RA	RCI
Device criticality classification	ACI	R
Scheduling automated patching (workstations/servers)	RA	CI
Validating business context prior to patch schedule implementation	ACI	R
Technical support during patch deployment	RA	CI
Patch roll-back procedure (to the extent reasonably possible)	RCI	RA
Notification of new devices needing onboarding	CI	RA
Notification of devices needing decommissioning	CI	RA
Monthly Executive Reporting	RA	CI

Task: Vulnerability Scanning	Cyvatar	Member
Installation of vulnerability agent	RA	CI
Configuration of vulnerability scanner/agent	RA	CI
Maintenance of vulnerability scanner/agent	RA	CI
Change Management	CI	RA
Provide list of potential target assets	CI	RA
Provide list of assets to be specifically excluded	CI	RA
Scheduling of on-going automated vulnerability scanning (internal, external, and/or cloud environments)	RA	CI
Technical validation of remediation efforts (to the extent reasonably possible)	RA	CI
Tracking of new, remediated, and persisted vulnerabilities	RA	CI
Provide Assessment Findings	RA	CI
Monthly Executive Reporting	RA	CI

Task: Non-Patch Related Remediation	Cyvatar	Member
Tracking of new, remediated, and persisted vulnerabilities	RA	CI
Misconfigurations remediation (to the extent reasonably possible)	RA	CI
End of Life Software/Operating Systems remediation	CI	RA
TLS/SSL Secure Communication Protocols remediation	CI	RA
Lead remediation efforts until identified gaps are remediated (to the extent reasonably possible)	RA	CI
Technical validation of remediation efforts (to the extent reasonably possible)	RA	CI

Secure Endpoint Management (SEM)

Task ownership is outlined below using the RACI Model.

Task: Endpoint Antivirus Security	Cyvatar	Member	MDR
Installation of Endpoint Security Agent	RCI	RA	N/A
Configuration of Endpoint Security Agent	RA	CI	N/A
Maintenance of Endpoint Security Agent	RA	CI	N/A
Change management	CI	RA	N/A
Review of security events	RA	CI	N/A
Management of groups	RA	CI	N/A
Management of policies	RA	CI	N/A
Monthly Executive Reporting	RA	CI	N/A

Task: Managment Detection & Response (MDR)	Cyvatar	Member	MDR
Initiate onboarding to 24x7x365 MDR Service	RACI	CI	R
24x7x365 monitoring	ACI	CI	R
Initial Incident Identification & Analysis	ACI	CI	R
Initial Incident Investigation, Triage, & Classification	ACI	CI	R
Threat Notification and Escalation	RACI	CI	R
Initial Threat Response (Actions: quarantine, kill, windows roll-back, remediate, & disconnect)	RACI	CI	R
Post-Mortem Analysis	CI	RA	CI
Escalate to an External Incident Response & Forensic Investigation*	CI	RA	CI

*Incident Response Retainer available for purchase separately

Cloud SaaS Security Management (CSM)

Task ownership is outlined below using the RACI Model.

Task:	Cyvatar	Member
Installation of CSM solution	RCI	RA
Configuration of CSM solution	ACI	R
Management of CSM solution	RA	CI
Change Management	CI	RA
Rule creation	RA	CI
Rule tuning	RA	CI
Alert tuning	RA	CI
Alert triage	RA	CI
Lead alert remediation efforts (to the extent reasonably possible)	CI	RA
Technical validation of remediation efforts	RA	CI
Monthly Executive Reporting	RA	CI

Managed Security & Awareness Training (SAT)

Task ownership is outlined below using the RACI Model

Task:	Cyvatar	Member
Provide list of users for enrollment	CI	RA
Enrollment of SAT solution	RA	CI
Configuration of training plan	RA	CI
Configuration of phishing campaigns	RA	CI
Management of SAT solution	RA	CI
Change Management	CI	RA
Continuous review of completion logs	RA	CI
Monthly Executive Reporting	RA	CI

Incident Response Management (IRM)

Task ownership is outlined below using the RACI Model.

Task:	Cyvatar	Member	Incident Response Team
Solution onboarding	RACI	CI	R
Escalation to Incident Response team for forensic investigation	CI	RA	CI
Initial investigation assistance and direction including clarification of the potential scope of the investigation	CI	CI	RA
Remote Response - by phone or email, within 8 hours of an Incident Report being submitted by the Customer	CI	CI	RA
Onsite Response* – dispatched and in route within 3 Business Days of an Incident Report being opened by Arista during Business Hours to pre-agreed locations in the U.S., Canada and the United Kingdom	CI	CI	RA
Forensic system and log analysis	CI	CI	RA
Assistance with providing data or logs from Cyvatar managed tools	RA	CI	RCI
Ongoing status reporting during the Incident	CI	CI	RA
Evidence collection and support	CI	CI	RA
Initiate request to utilize remaining Digital Forensics and Incident Response Retained Services hours for alternative Services	CI	RA	CI
Management of IRM solution	RA	CI	RCI
Change Management	CI	RA	CI
Detailed technical report and executive presentation based on the findings and recommendations as a result of the incident analysis	CI	CI	RA

*Travel Expenses and additional fees may apply.

Multifactor Authentication (MFA)

Task ownership is outlined below using the RACI Model.

Task:	Cyvatar	Member
Provide list of users and hosts for enrollment	CI	RA
Installation of MFA solution	RA	CI
Configuration of MFA solution	RA	RCI
Management of MFA solution	RA	CI
Change Management	CI	RA
Rule creation	RA	CI
Rule tuning	RA	CI
Monthly Executive Reporting	RA	CI

Email Security Management (ESM)

Task ownership is outlined below using the RACI Model.

Task:	Cyvatar	Member
Provide list of email domains	CI	RA
Configuration of ESM solution	RA	CI
Management of ESM solution	RA	CI
Change Management	CI	RA
Monthly Executive Reporting	RA	CI

DNS Security Management (DSM)

Task ownership is outlined below using the RACI Model.

Task:	Cyvatar	Member
Installation of DSM solution	RCI	RA
Provide list of whitelisted pages	RCI	RA
Configuration of DSM solution	RA	RCI
Management of DSM solution	RA	CI
Whitelist approvals	CI	RA
Change Management	CI	RA
Monthly Executive Reporting	RA	CI

Mobile Threat Defense (MTD)

Task ownership is outlined below using the RACI Model.

	Cyvatar	Member
Installation of MTD solution	RCI	RA
Configuration of MTD solution	RA	CI
Management of MTD solution	RA	CI
Change Management	CI	RA
Monthly Executive Reporting	RA	CI

CYVATAR.AI

The Future of Cybersecurity.

Questions? Contact
support@cyvatar.ai