



# RACI Solutions Strategy Overview

Bringing People, Process, and Technology  
to Streamline Your Cybersecurity Program



# Table of Contents

Roles and Responsibilities.....	3
Threat & Vulnerability Management (TVM).....	4
Secure Endpoint Management (SEM).....	6
Cloud SaaS Security Management (CSM).....	8
Identity Access Management (IAM).....	9
IT Asset Management (ITAM).....	10
Managed Security & Awareness Training (SAT).....	11



# 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 process or task being completed appropriately*

**C****Consulted**

*People who are not directly involved with carrying out the task, but who are informed*

**I****Informed**

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



# Threat & Vulnerability Management (TVM)

Cyvatar's Threat & Vulnerability Management Subscription continuously identifies, assesses, classifies, remediates, and mitigates security weaknesses. Additionally, it provides understanding of root cause analysis to address potential flaws in policy processes.

Task ownership is outlined below using the RACI Model.

Task: Patch Management	Cyvatar	Member
Solution evaluation & onboarding	RA	CI
Installation of patch management system	ACI	R
Configuration of patch management system	RA	CI
Maintenance of patch management system	RA	CI
Change management	CI	RA
Issue review and resolution	RA	CI
Device Inventory (classification of assets)	ACI	R
Scheduling automated patching (workstations/servers)	RA	CI
Technical validation of patches prior to implementation (to the extent reasonably possible)	RA	CI
Validating business context prior to patch implementation	ACI	R
Patch roll-back procedure	RA	CI
Technical support during patch deployment	RA	CI
Monthly Executive Report Card	RA	CI



Task: Vulnerability Scanning	Cyvatar	Member
Solution evaluation & onboarding	RA	CI
Build virtual vulnerability scanner	RA	CI
Installation of virtual vulnerability scanner	ACI	R
Installation of vulnerability agent	ACI	R
Configuration of vulnerability scanner/agent	RA	CI
Maintenance of vulnerability scanner/agent	RA	I
Change Management	CI	RA
Provide list of potential target assets	ACI	R
Provide list of assets to be specifically excluded	ACI	R
Scheduling of on-going automated vulnerability scanning (internal, external, and/or cloud environments)	RA	CI
Notification of ports open to the internet (Cyvatar Port Zero)	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 Report Card	RA	CI

Task: Non-Patch Related Remediation	Cyvatar	Member
Development of remediation plan and schedule	RA	CI
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)

Cyvatar's Secure Endpoint Management Subscription provides a fully managed AI-based antivirus solution. The goal is to proactively secure endpoints from malware attacks and move them to a preventative state so that it blocks malware attacks before they can execute, as opposed to detect and respond. This is combined with 24/7/365 monitoring for attacks by a Managed Detection and Response service.

Task ownership is outlined below using the RACI Model.

Task: Endpoint Antivirus Security	Cyvatar	Member	MDR
Solution evaluation & onboarding	RA	CI	N/A
Installation of Endpoint Security Agent	ACI	R	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 Report Card	RA	CI	N/A



Task: Management Detection & Response (MDR)	Cyvatar	Member	MDR
Initiate onboarding to 24x7x365 MDR Service	A	CI	R
24x7x365 monitoring	A	CI	R
Initial Incident Identification & Analysis	ACI	CI	R
Initial Incident Investigation, Triage, & Classification	ACI	CI	R
Incident Notification and Escalation	RACI	CI	R
Initial Incident Mitigation & Response (Actions)	RI	ACI	R
Escalated Incident Response & Investigation	I	RA	CI
Escalated Incident Forensic Analysis	I	RA	CI
Post-Mortem Analysis	I	RA	CI



# Cloud SaaS Security Management (CSM)

Cyvatar's Cloud Security SaaS Management Subscription provides the visibility needed to detect and investigate breaches, uncover insider threats, and secure the most commonly used SaaS applications like Salesforce, Zoom, Office 365, AWS, Slack, G-Suite, Azure and more.

Task ownership is outlined below using the RACI Model.

Task: Patch Management	Cyvatar	Member
Solution evaluation & onboarding	RA	CI
Installation of CSM solution	ACI	R
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
Gap and risk assessment based on security best practices	RA	CI
Development of remediation plan and schedule	RA	CI
Lead remediation efforts until identified gaps are remediated (to the extent reasonably possible)	RAI	RCI
Technical validation of remediation efforts (to the extent reasonably possible)	RA	CI
Monthly Executive Report Card	RA	CI





# Identity Access Management (IAM)

Cyvatar's Identity Access Management Subscription makes it harder for attackers to penetrate networks and obtain account access. Helps prevent credential compromise. Adds protection to individuals by controlling access to applications through an additional verification capability.

Task ownership is outlined below using the RACI Model.

Task: Patch Management	Cyvatar	Member
Solution evaluation & onboarding	RA	CI
Provide list of users and hosts for enrollment	ACI	R
Enrollment of IAM solution	RA	CI
Configuration of IAM solution	RA	CI
Management of IAM solution	RA	CI
Change Management	CI	RA
Rule creation	RA	CI
Rule tuning	RA	CI
Monthly Executive Report Card	RA	CI



# IT Asset Management (ITAM)

Cyvatar's IT Asset Management Subscription helps you gain a comprehensive asset inventory in a cloud-managed solution. Integrates with over two hundred security and management solutions to discover assets and provide contextual information about each asset. Identifies security coverage gaps and helps remediate them.

Task ownership is outlined below using the RACI Model.

Task: Patch Management	Cyvatar	Member
Solution evaluation & onboarding	RA	CI
Installation of ITAM solution	ACI	R
Configuration & Integration of ITAM solution	ACI	R
Management of ITAM solution	RA	CI
Change Management	CI	RA
Provide inventory list of hardware and software assets within environment	ACI	R
Identification of assets with missing or malfunctioning agents, assets not being scanned for vulnerabilities, managed/un-managed devices and rogue devices on privileged networks	RA	CI
Gap and risk assessment based on security best practices	RA	CI
Remediation recommendations	RA	CI
Development of remediation plan and schedule	RA	RCI
Lead remediation efforts until identified gaps are remediated (to the extent reasonably possible)	RAI	RC
Technical validation of remediation efforts (to the extent reasonably possible)	RA	CI
Monthly Executive Report Card	RA	CI



# Managed Security & Awareness Training (SAT)

Cyvatar's Managed Security & Awareness Training Subscription keeps cybersecurity top of mind for employees by embedding continuous and relevant training in the right places at the right time. Users learn through actions and increase both awareness and knowledge over time with real time training, actionable metrics based on training, and customized education based on your company's unique culture. What's more is security and awareness training is managed for you, so you won't need to worry about a thing.

Task ownership is outlined below using the RACI Model

Task: Patch Management	Cyvatar	Member
Solution evaluation & onboarding	RA	CI
Provide list of users for enrollment	IC	RA
Enrollment of SAT solution	IC	RA
Configuration of SAT solution	RA	IC
Management of SAT solution	RA	IC
Change Management	IC	RA
Identify risks and gaps	RA	IC
Create training and assessment plan	RA	IC
Continuous review of completion logs	RA	IC
Provide recommendations for remediation on risks and gaps identified	RA	IC
Develop a remediation plan and schedule	RA	RC
Lead the remediation efforts with a weekly meeting cadence until identified gaps are remediated (to the extent reasonably possible and approved by Member)	RA	RC
Monthly Executive Report Card	RA	IC



# CYVATAR<sup>.AI</sup>

Effortless Cybersecurity.

Reach us at anytime at  
[Cydekicks@cyvatar.ai](mailto:Cydekicks@cyvatar.ai)