DATA SHEET

Cymulate Cowork

Command the Swarm for Cyber Defense Engineering

Security teams do not lack data. They lack time, coordination and scalable expertise to turn threat intelligence, validation results, exposures and control telemetry into action. Too often, critical workflows depend on swivel-chair operations across security tools, manual analysis and follow-up that often arrives too late to reduce risk.

Cymulate Cowork is an agentic SaaS extension to the Cymulate Platform. Powered by Vero AI, Cymulate Cowork integrates exposure validation into autonomous, repeatable workflows for agentic cyber defense engineering.

With plain-language prompts and recurring scheduled workflows, Cymulate Cowork assembles the right agents, skills and trusted integrations that gather context, analyze risk, create assessments, validate security and drive action across Cymulate and the broader security ecosystem. Command your AI swarm to continuously prove and improve cybersecurity.

A New Operating Model Powered by Vero AI

Built on Cymulate Vero AI, Cymulate Cowork gives security teams a command interface for autonomous execution. Instead of manually collecting data, stitching together workflow steps and checking outcomes one by one, teams operationalize repeatable cyber defense engineering processes with consistent execution.

Users define an objective, and Cymulate Cowork assembles a goal-oriented squad that combines agents, skills, context and integrations to complete the tasks and ultimate goal.

Agents analyze the current state, plan and execute actions, collaborate when needed and determine when an objective has been met. Cymulate Cowork includes prebuilt agents and lets users create their own.

Skills capture the Cymulate security engineering and offensive testing expertise, providing knowledge and logic that agents use to complete tasks.

Routines automate recurring workflows that execute a known sequence of steps to achieve a cyber defense engineering goal. Cymulate Cowork includes prebuilt routines and lets users build custom routines to their processes.

Benefits

Act beyond the platform

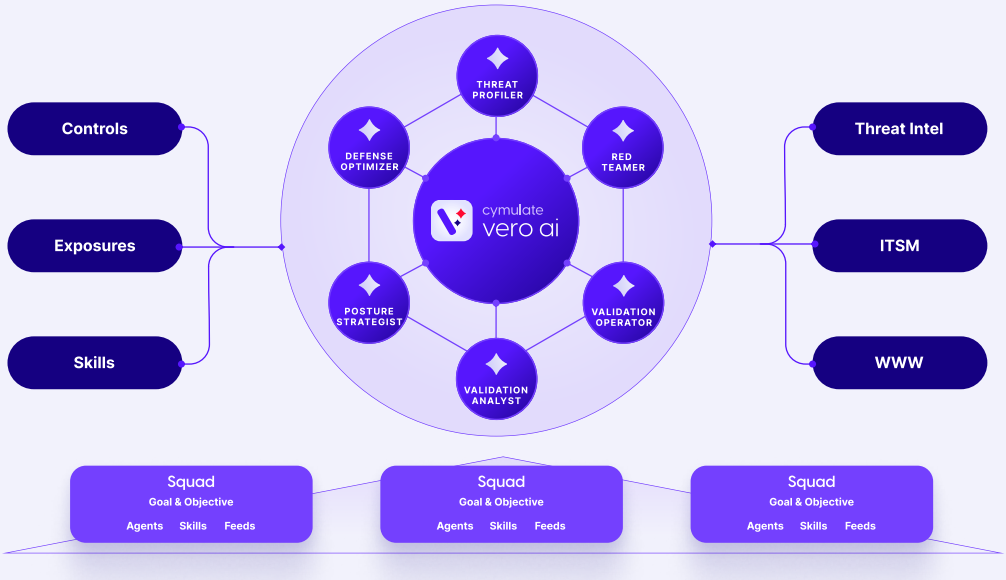
Orchestrate work across Cymulate, SIEM, EDR, ticketing, threat intel, vulnerability management and team collaboration tools.

Automate recurring workflows

Turn repeatable tasks into reusable routines that run on demand, on a schedule or with approval.

Scale expertise, not headcount

Extend your team's capabilities with expert-built agents, skills and routines.



Trusted Integrations Across the Security Ecosystem

Cymulate Cowork is designed to work across the systems that shape cyber defense decisions and actions. Through trusted integrations, Cowork can gather information, correlate findings and support next steps across:

- Security controls such as SIEM, EDR, WAF, firewalls, IPS, email gateways and web gateways
- Threat intelligence and public data sources such as CERT advisories, CVE/KEV feeds, NIST and compliance frameworks
- Exposure and vulnerability data sources
- ITSM and ticketing platforms
- Team collaboration platforms such as Slack and Microsoft Teams

By connecting these systems to the Cymulate validation engine, Cymulate Cowork helps teams move from disconnected data to coordinated action.

Ready-to-Use Routines for Autonomous Cyber Defense

In addition to custom, user-built routines, Cymulate Cowork includes prebuilt routines that help teams automate cyber defense workflows from day one. Examples include:

- **Emerging threats and CERTs –** Collect third-party threat intel and CERT advisories, analyze relevance to the environment, map attack scenarios and prepare tailored assessments
- **CVE and KEV awareness –** Monitor external CVE and KEV updates related to the environment, score exposure based on validation results and create follow-up actions when risk thresholds are met.
- **Mitigation validation –** Re-run the original attack scenario when mitigation tasks are closed to confirm the issue is actually fixed
- **Mitigation tracking –** Identify remediation tasks that are approaching or missing SLA targets and escalate them with supporting context
- **Daily assessment analysis –** Review the last 24 hours of assessment activity, summarize results and recommend the highest-value actions to improve security.
- **Detection engineering routines –** Monitor new or changed SIEM rules, map them to attack scenarios and validate whether detections still work as expected (requires Cymulate Detection Studio)

Why Choose Cymulate?

Complete threat coverage

The most comprehensive threat library that enables validation across the full attack lifecycle – plus daily updates for the latest threats.

AI-powered environment and context mapping

AI personalizes what to test, what matters and what to do next based on your assets, industry, controls, and exposures.

Defense engineering control plane

A closed-loop system that turns validation into continuous improvement across controls and threat detection.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.