Preparing for Mythos and Future AI-Driven Threats

Security readiness brief on AI-augmented attacker capabilities

AI Driving the Need to Shift Approaches

AI is reaching a turning point in cybersecurity, transforming vulnerability discovery and exploitation into automated, scalable processes. Systems like Mythos can identify weaknesses and execute complex attacks with minimal human input, dramatically lowering the cost and expertise required. As these capabilities spread, static defenses will become ineffective, and organizations must urgently shift to adaptive, resilience-focused security strategies to address the emerging AI-driven threat landscape.

Where Mythos-class Capability Lands Hardest

Internet-facing Attack Surface
Public web apps, exposed APIs, cloud endpoints, and SaaS misconfigurations are first to be probed when reconnaissance and exploitation costs collapse.

Legacy and Unmaintained Code
Vendor software, embedded systems, and dormant CVEs in production code carry years of latent risk that AI-driven discovery can now monetize quickly.

Identity and Entitlement Sprawl
Over-permissioned access, weak segmentation, and standing privileges turn any initial foothold into broad lateral movement and data access.

AI and LLM Data Exfiltration Paths
Copilot, Gemini, and third-party LLM use without proper data classification and access governance create new, fast-moving exfiltration channels.

EchoStor Strategic Service Offerings

MSSP / Managed Security Services

OPTION A	OPTION B	OPTION C
Targeted Mythos Readiness Bundle	Strategic vCISO Partnership	Cybersecurity Advisory Hours
• External Pen Test • AI / LLM Exfiltration Assessment • Executive risk readout and 90-day action plan	• Continuous executive security leadership tied to a multi-quarter Mythos readiness roadmap	• Flexible 40/80/160-hour blocks drawn down as questions and decisions surface

EchoStor Technology Partners Leading the Charge (Project Glasswing)

aws	BROADCOM	CISCO	COHESITY	CROWDSTRIKE
Microsoft	NVIDIA	paloalto	rubrik	zscaler

EchoStor Tactical Offerings

Early Identification

External + Internal Pen Testing
Web App + API Pen Testing
Cloud Security (AWS, Azure, GCP)
Vulnerability Management + Scanning
Wireless Security Assessment

Contain Blast Radius

Zero Trust Assessment + Enablement
IAM Assessment + Cleanup
SIEM / SOAR Implementation
PKI + Certificate Lifecycle
Network Segmentation Review

Govern the Program

vCISO Advisory
Security Risk Assessment
Compliance Gap Assessment
Maturity Measurement + Planning
Tabletop Excercises

Protect the Data

DLP / DSPM Assessment
AI / LLM Exfiltration Assessment
Data Classification Design
Purview + CASB Implementation
Remediation + Tooling Deployment

Continue the Conversation

Get in touch

EchoStor Security Team:
security-team@echostor.com