DISPEL

Claude Mythos & OT Cybersecurity Risk

Modern risk and how its impacting utilities, manufacturing, and energy CISOs

What Is Claude Mythos?

Released in April 2026, Claude Mythos is an AI model that outperforms human experts at finding and exploiting software vulnerabilities. It has identified thousands of high-severity flaws across major operating systems and browsers — including one dormant for 27 years — and can chain those findings into working exploits with minimal human involvement.

Speed Is The Threat, Not Sophistication
Mythos doesn't make OT attacks more sophisticated — it makes them dramatically faster and more accessible. Your adversary no longer needs advanced expertise. They need an exposed endpoint, a default password, and motivation. Mythos handles the rest.

How This Changes OT Security

Security teams and CISOs already understand the threat landscape. What Mythos changes is the speed and accessibility of exploitation, particularly in OT environments where the conditions for abuse already exist.

The Entry Points Already Exist

CISA confirms threat actors are already present in OT environments — not through novel exploits, but through the pathways used every day: internet-exposed services, shared credentials, and unmanaged third-party access. IT/OT convergence has extended this exposure deep into legacy systems never designed for network connectivity.

How Mythos Moves Through Your OT Environment

AI is exceptional at pattern matching and replication. In flat OT networks running legacy equipment, adversary spread is structurally hard to control. Mythos accelerates every phase:

- **Rapid environment mapping**— scans for exposed endpoints and default credentials at machine speed across thousands of similar environments simultaneously
- **Exploit chaining**— automates progression across IT/OT boundaries, covering tracks in real time
- **Credential mimicry**— uses valid credentials to mirror routine vendor operations, making detection far harder

The CISO's core question: "If an attacker authenticated as one of your vendors — from the right IP, with the right credentials — how long before you'd know? Would you be able to prove it wasn't that vendor?" CISA's advisory on the Iranian campaign illustrates exactly this: attackers used valid credentials to blend into legitimate operations. Mythos amplifies this at scale.

SANS ICS Critical Controls most directly implicated are Control 2 (Defensible Architecture) and Control 4 (Secure Remote Access) — both of which Dispel is purpose-built to address.

50%
of industrial incidents begin with unauthorized external access
SANS ICS/OT Security 2025

30%
OT cyber risk reduction from secure remote access + defensible architecture
Dragos Financial Risk Report 2025

$170K
average cost per hour of unplanned OT downtime
ABB Modernization for Resilience 2025

DISPEL

How Dispel Closes The Gap In OT Security

Dispel doesn't rebuild your OT security program. It hardens your defensive posture where it matters most: access, trust, and control — combining defensible architecture, dynamically risk-scored remote access, and session-level visibility into a single deployable security layer, live in hours.

Just-in-Time Access Windows

If the pathway doesn't exist, Mythos cannot traverse it. Dispel establishes access paths only when needed and only for the duration of an approved, audited session — then tears them down automatically. There are no persistent VPN tunnels to exploit, no always-on connections to pivot through.

Addresses: SANS Control 4 — Secure Remote Access

Disposable Infrastructure

Connecting directly from a laptop gives AI-driven malware somewhere to land and spread — a persistent endpoint to pattern-match across. Dispel eliminates that by routing every session through an ephemeral intermediary, Virtual Desktop Infrastructure (VDI) or Browser Connect, automatically wiped at session end. Think surgical gloves: you don't carry them between operating rooms. Fresh pair, do the work, discard. Every session runs the same way. And that constant cycle of destruction and rebuild is what powers Dispel's Moving Target Defense — the network is always moving because the infrastructure never stands still.

Addresses: SANS Control 2 — Defensible Architecture

Identity, Intelligence, and Session Forensics

Knowing someone authenticated is not the same as knowing it was really them. Organizations can now extend the authentication chain with Dispel Intelligence Session Forensics and risk scoring — across every OT remote access session in real time across identity, activity, and behavior— mitigating modern AI threats and minimizing administrative friction.

On Information: Siloed information is dead information. Too much information is useless information. Dispel packages composite risk and delivers it to the right people — your security team for intervention, and your access window approvers for the moment to call the vendor and confirm.

Addresses: SANS Control 4 — Secure Remote Access

About the Dispel Platform

The Dispel Zero Trust Engine securely connects people and OT data across complex OT environments, unifying OT Secure Remote Access and Industrial Data Streaming to remove legacy access friction so operations can move faster without increasing risk.

Ready to take the first step toward unified operations with Dispel?

Book a demo today.

dispel.com/book

DISPEL