Bell Integration
Ambitious Transformation

EBOOK

Claude Mythos: From Risk to Resilience

Your blueprint to defend, detect, respond and adapt to uncertainty

Navigating AI-enabled Enterprise Cyber Security Challenges

For business leaders driving critical infrastructure, the arrival of frontier AI models like Anthropic's Claude Mythos Preview has fundamentally altered the threat landscape, reducing the window between vulnerability discovery and weaponisation to near zero.

Government agencies, regulators and critical infrastructure sectors, with banking and financial services a priority, have collaborated to evaluate systemic risks and mitigate the potential for zero-day exploits.

Bell's Cyber Security and AI experts have shaped this blueprint to help you upgrade security and strengthen resilience. The blueprint offers a practical guide on upgrading your security posture and where Bell can offer additional support to strengthen your resilience when Mythos 5 or similar models emerge in the future.

Where historically organisations could tolerate longer remediation cycles, this dynamic is shifting. Vulnerabilities that may never have been exploited in the past now have a higher likelihood of being weaponised, including lower-severity issues that can be combined into attack chains.

This has material implications for both security teams and business risk. Slower patch cycles and resource constraints increasingly translate into real exposure.

For security leaders, identifying vulnerabilities is only part of the equation. Have you thought about how you will defend, detect, respond and adapt to this looming uncertainty?

From a cyber security perspective, this means:

Before Mythos

- Longer patch cycles were often acceptable.
- Many vulnerabilities were never practically exploited.
- Vulnerability management was sometimes treated as a compliance-driven activity.

After Mythos

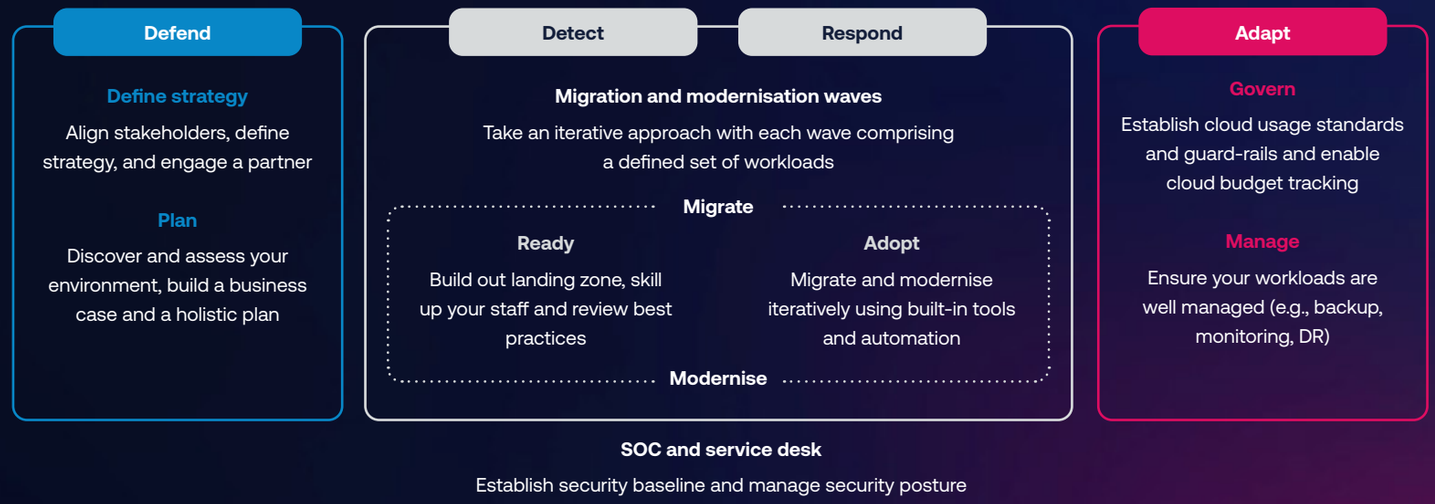
- Time to exploitation is significantly reduced.
- Lower severity vulnerabilities can be chained into meaningful attacks.
- Remediation speed becomes critical to reducing risk exposure.
- Security teams face increased volume and complexity of findings.

This blueprint is your practical guide on upgrading your cyber security posture and shows you where Bell can offer our expertise and solutions to **strengthen your cyber resilience**, when Mythos 5 or similar models emerge in the future.

Achieve true cyber resilience as you defend, detect, respond and adapt

Designed to give organisations all the coverage they need, Bell Integration's cyber security services enable you to build a robust defence against cyber threats without having to make extensive investments in hardware or specialised staff.

We help you to proactively manage risks across an ever-expanding enterprise perimeter, so you can protect your most valuable assets and operate in a truly digital way.



Sharpen your Defences

Actionable steps for your organisation

- Prioritise robust foundational cyber security capabilities, including zero trust architecture, strict network segmentation, and phishing-resistant multifactor authentication (MFA).
- Aggressively reduce legacy technical debt.
- Implement a Shift Left strategy.

Bell can help you by:

- Assessing existing cyber security maturity levels against industry frameworks such as ISO 42001, NIS2 and others to identify gaps and define strategy.
- Leading legacy modernisation and cloud transformation initiatives.
- Moving your infrastructure to platforms that offer improved security visibility, control, and a reduced attack surface.
- Providing advisory and consultancy services to educate your board, frame the risk, and redesign your security operating model. This include Maturity Assessments.
- Orchestrating an architecture redesign driven directly by your risk exposure, ensuring your defences are structurally prepared for the AI era.

Further reading

- "Anthropic Allows Glasswing Partners to Share Mythos-Based Findings - Security Boulevard"
- "The Cybersecurity Implications of Claude Mythos and OpenAI Cyber"
- "Project Glasswing Just Made Your Security Playbook Obsolete - BankInfoSecurity"
- "Claude Mythos and the AI Cybersecurity Wake-Up Call | Bain ..."
- "Anthropic's 'Project Glasswing' Exposes the Next Challenge for Vulnerability Management"
- "Project Glasswing Just Made Your Security Playbook Obsolete - BankInfoSecurity"

Detect Early

Actionable steps for your organisation

- Organisations must transition to anomaly detection focused on unusual behavioural patterns.
- Establish a dedicated AI threat “war room” to systematically probe your own systems using the same advanced tools adversaries employ.
- Move away from periodic vulnerability scanning toward continuous, adversary-style testing that validates the actual exploitability of applications and cloud configurations, using AI agents to trace reachable vulnerabilities.

Bell can help you by:

- Driving AI-powered DevSecOps transformation.
- Embedding automated testing and scanning directly into your CI/CD pipelines to catch vulnerabilities early.
- Providing Intelligent Managed Services (24x7 security operations), driven by AI insights, enabling continuous vulnerability monitoring and triage.
- We ensure your organisation can manage and interpret the massive volume of vulnerability data surfaced by tools like Mythos.

Further reading

- “Claude Mythos and the AI Cybersecurity Wake-Up Call | Bain ...”
- “The Cybersecurity Implications of Claude Mythos and OpenAI Cyber”

Respond with Speed

Actionable steps for your organisation

- Compress patch timelines by adopting high-automation patching and “safe auto-remediation”.
- Deploy engineering-owned testing harnesses, canary releases, and rapid rollback playbooks so you can deploy emergency fixes in hours without breaking production.

Bell can help you by:

- Understanding your organisation’s operational MVP, and ensuring that these assets are prioritised in resilience planning.
- Deploying high-volume vulnerability remediation programs using a SWAT team approach.
- Providing code refactoring and patching at scale, automating patch validation to help you remediate exposures before they are exploited.
- Implementing Incident Response retainers to restore the business in the event of an incident.
- Providing Intelligent Managed Services for machine speed monitoring, detection, decision and action.

Further reading

- “Anthropic’s ‘Project Glasswing’ Exposes the Next Challenge for Vulnerability Management”
- “Project Glasswing Just Made Your Security Playbook Obsolete - BankInfoSecurity”
- “The Cybersecurity Implications of Claude Mythos and OpenAI Cyber”
- “Claude Mythos and the AI Cybersecurity Wake-Up Call | Bain ...”

Adapt to Future-proof

Actionable steps for your organisation

- Continuously test your systems against severe but plausible disruption scenarios, mapping third-party and open-source supply chain dependencies.
- Treat these ‘fire drill’ events as permanent, board-level business risk rather than an isolated IT issue, fundamentally redesigning operational defence.

Bell can help you by:

- Transitioning from short-term tooling implementations to continuous, multi-year operating model transformations.
- Embedding AI-powered security into your development lifecycle, enabling continuous, secure delivery that adapts to emerging threats.
- Acting as a strategic orchestrator across AI, cloud, and security to ensure your organisation possess the long-term operational resilience required to withstand the industrialised exploitation of the frontier AI era.

Further reading

- Chapter 03: Keeping pace with evolving technology | National Cyber Security Centre
- Critical Infrastructure Cybersecurity Guide | Security Insider
- “Operational resilience: insights and observations one year on - FCA”

Managed Services

Financial regulators globally are moving beyond point-in-time compliance toward continuous operational resilience. Authorities including the SEC, FRB and NYDFS (US), FCA and the Bank of England (UK), ESAs and ECB (EU), and the CBUAE and VARA (UAE) are mandating that firms actively plan for and mitigate cyber risk, strengthen resilience, and address emerging threats such as frontier AI-driven attacks.

Our end-to-end adaptive cyber security services enable you to outsource all or part of your cyber security function. In addition to an extensive suite of managed services that release your IT teams from having to do any heavy lifting, our comprehensive offerings also include cyber security strategy and advisory services that help you strengthen your defences and improve your security posture, identify and manage risks, and comply with regulations.

Bell's Managed Vulnerability Management Service enables organisations to keep pace by operationalising visibility, prioritisation, and remediation into a continuous, risk-led process.

It provides continuous visibility of security weaknesses across your IT estate, combining automated discovery with expert analysis to help organisations understand their exposure, prioritise risks that matter, and take effective action to reduce cyber threats.

Bell's Penetration Testing as a Service (PTaaS) capability provides you with a continuous validated view of your attack surface, allowing us to **Find, Fix and Verify vulnerabilities across the enterprise** as part of the service.

Bell can help you to strengthen your ongoing security operations. Talk to us today.

Vulnerability Management Service Features

- Vulnerability Management Platform (Deployment & Management)
- Regular Scanning & Monitoring (On-prem, Cloud, Hybrid)
- Ad-hoc Scanning
- Vulnerability Evaluation (Validation & Enrichment)
- Risk-based Vulnerability Prioritisation
- Actionable Remediation Guidance
- Dashboards & Reporting
- Service Performance Reporting & Reviews
- Telephony Support for Enhanced Remediation Guidance
- Enhanced Remediation Governance
- IoT / OT Vulnerability Support (Optional Add On)

Strengthen your cyber resilience with Bell Integration

From endpoint security to cyber defence, cloud and workplace security solutions, we ensure you're able to wrap protection around every user, every device and every connection.
We help you to proactively manage risks across an ever-expanding enterprise perimeter, so you can protect your most valuable assets and operate in a truly digital way.

Get in touch with us today.
www.bell-integration.com/cyber-security
+44 2392 825925

About Bell Integration

Bell Integration is a global technology leader that partners with customers to create lasting, ambitious digital transformation.

We are our customer's accelerator – orchestrating the right partners, systems, and ideas to create measurable impact.

Bell Integration brings over 30 years of trust, expertise, and innovation to the table, evolving from an independent UK-based business to a global powerhouse.

With talented teams operating across continents, we support the full IT life cycle from strategic consulting to project design and delivery.

See how Bell Integration can help your business succeed. Please contact us on marketing@bell-integration.com or visit www.bell-integration.com.