Cloud Cybersecurity Consulting

End-to-end security for cloud migration, existing architectures and hybrid environments.
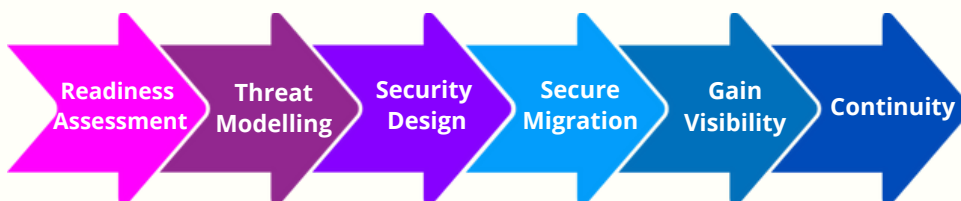
What is Cloud Cybersecurity Consulting?

Cloud Cybersecurity Consulting is an end-to-end cloud security service offering design, assurance, and operations consulting. Domain experts with years of <u>nation-state-grade</u> experience identify security gaps, prioritize risks and develop defense plans to create sustained cloud security with continuous automated controls.

The program matures every part of the organization's cloud infrastructure to be more secure and resilient to cyber threats while at the same time encouraging flexibility, growth, and productivity.

Whether the enterprise is migrating its systems to the cloud from scratch, working in hybrid or "cloud first" environments, or developing its own cloud applications, this service will protect your data and infrastructure both now and in the future.

How does Cloud Cybersecurity Consulting work for me?

There are typically six stages in the engagement. HolistiCyber delivers best-practice consulting at each stage:

Readiness Assessment → Threat Modelling → Security Design → Secure Migration → Gain Visibility → Continuity

Our domain experts have years of experience securing cloud infrastructures for large enterprises in major industries such as utilities, software companies, banking, and financial services. The cloud journey often begins by accompanying the organization's first adoption of cloud infrastructure and the entire process through design and assurance. Other times, we have provided support for strategic cloud initiatives which include:

- Cloud security framework guidance
- Cloud security assessments
- Holistic consulting for organizational structure
- Cloud environment penetration tests
- Cloud environment Red-team/ Blue-team simulations

We have helped customers secure their cloud environments in AWS, Azure, Google Cloud, Microsoft 365 and all main applications in the enterprise.

WHAT SHOULD YOU EXPECT?

- **Strategy roadmap - productive, concise, and prioritized, to meet current and future needs.**

- **Risk and readiness assessments (Mapping the company's current threat landscape and security posture).**

- **Threat modeling**

- **Cloud security design**

- **Cloud risk mitigation**

- **Visibility and continuity**

- **Ongoing support of strategic cloud initiatives**

- **Implementation of governance and compliance.**

- **Zero overhead for clients, fully managed service.**

- **Policy outline adapted to unique company business needs, priorities, and risk appetite.**

- **Implementing effective risk controls.**

- **Clear prioritization of security threats that need to be handled immediately vs. items that do not pose an immediate risk.**
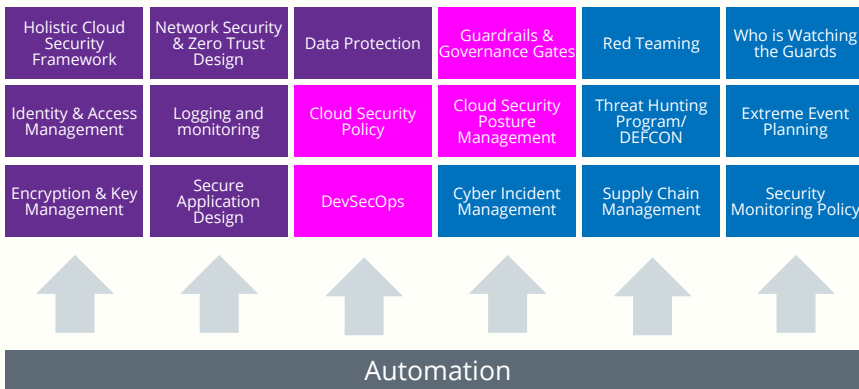
How can enterprises keep up with today's cyber threats? By getting ahead of them.

As cloud adoption increases across industries and sectors, malicious actors with nation-state-grade attack tools are spending more time and resources to attack cloud environments.
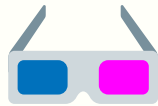
Given the amount of sensitive data inhabiting multiple cloud environments, the attack surface has expanded dramatically, leading to more significant threats, including the introduction of malware and data loss. Ensuring that enterprises have a proactive cloud security strategy is imperative. Our readiness assessments and threat modeling are focused on the company's specific attack surface and threat agents, determining the maturity of the company's security program and thereby producing informed cybersecurity risk management decisions to protect critical data and infrastructure.

The service delivers complete cloud security design based on company needs, and our experts work alongside the company's team to securely implement cloud migrations and create full cloud visibility for governance and compliance policies, as well as for ensuring continuity with processes, automation, and testing.
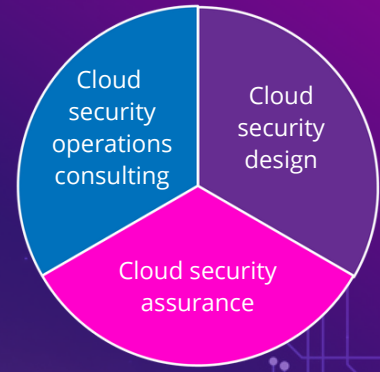
Cloud security operations consulting

Cloud security design

Cloud security assurance

What's in the cloud defense toolbox?

Holistic Cloud Security Framework	Network Security & Zero Trust Design	Data Protection	Guardrails & Governance Gates	Red Teaming	Who is Watching the Guards
Identity & Access Management	Logging and monitoring	Cloud Security Policy	Cloud Security Posture Management	Threat Hunting Program/ DEFCON	Extreme Event Planning
Encryption & Key Management	Secure Application Design	DevSecOps	Cyber Incident Management	Supply Chain Management	Security Monitoring Policy

Automation

"One of the reasons we like having HolistiCyber onboard is because they provide the expertise that would otherwise require hiring a large professional team to try to get the experience needed. In any case, it is almost impossible to assemble such a team, not to mention expensive. These folks provide knowledge, expertise, and excellent customer service."

CISO, Financial Institution, USA

Why HolistiCyber?

1. **Nation-state-grade expertise** - our staff of white-hat security experts is composed of former military and government offensive practitioners who can examine the attack surface from the vantage point of the attacker and not only from the company's vantage point. We have a solid grasp of the sophisticated tooling available to today's attackers and access to those attack tools.
2. **Holistic approach** - we tie compliance, remediation, and mitigation solutions to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.