

End-to-end Managed Security Services

Now with Managed Detection and Response (MDR) & Extended Detection and Response (XDR)



Bid farewell to outdated cybersecurity practices

With close to one hundred thousand online attacks occurring worldwide each day, cybercrime is the only proliferating global trend that every enterprise must stay away from. Instead of struggling to keep pace using outdated cybersecurity policies, organizations must upgrade to a new security posture that offers intelligent, round-the-clock protection.

Managed security services (MSS) from Cloud4C can help you accelerate end-to-end cybersecurity transformation on the cloud ranging from infra, datacenters and databases, platforms, software, workloads to apps, endpoints, IoT/Edge landscapes, other multiple clouds, and more.

Switch to intelligent security to combat advanced threats

To bolster continuity and future-ready growth while building resilience against the most advanced adversaries, Cloud4C leverages breakthrough AI-powered proprietary platforms, advanced cloud-native security tools, and transformative security automation solutions.

Cybersecurity-as-a-Service

- » Managed Cybersecurity solutions for public, private, hybrid/multi cloud platforms with ease
- » Embedded cloud-native solutions such as Azure Sentinel, Amazon Cloudwatch, etc.
- » Streamlined SaaS, IaaS, PaaS, CaaS security along with the entire cloud stack end-to-end

Our key differentiators

- » Security frameworks utilizing the MITRE ATT&CK, CIS Critical Security Controls, etc.
- » Comprehensive **24x7** monitoring program
- » Dedicated Cybersecurity Incident and Response (CSIRT) team
- » Threat Intelligence powered by Industry leading platforms (Microsoft, OSINT, STIX & TAXI, MISP)
- » **40+** Security Controls | **25+** Centres of Excellence | **2000+** global cloud experts
- » Proven experience in deploying and **managing robust SIEM**
- » **24x7** Proactive threat hunting
- » Industry specific Threat Intelligence
- » Next Gen SIEM Analytics with **AI** and **ML** & **SOAR**
- » Effective Incident Analysis and Response
- » Certified in **ITIL** and **COBIT**
- » We not only detect, rapidly respond to threats but also perform service improvements

Full breadth of Cloud4C's end-to-end Managed Security Services

Cloud4C Managed Detection and Response

Cloud4C's Advanced Managed Detection and Response (MDR) service a necessary cybersecurity revolution that addresses the threat management lifecycle end-to-end with advanced automation and intelligence. This advanced MDR service helps organizations detect and respond to advanced threats before they impact the business.

- » End-to-end threat hunting, threat discovery, risk analysis, and threat response solutions & managed services
- » Monitor IT assets in real-time, secure endpoints with Endpoint Detection and Response, embed cutting-edge AI/ML analytics
- » Agile threat management lifecycles with multi-cloud support



Endpoint Detection and Response (EDR)

- » Cloud4C EDR services are predictive and focus on identifying advanced persistent threats and never before-seen malware that are designed to evade traditional security defenses
- » Helps in conducting an extensive root cause analysis and aid with faster incident response
- » Combined power of cyber threat intelligence, machine learning capabilities and advanced file analysis helps to detect advanced threats

End-to-End Intelligent Enterprise Protection

- Threat Monitoring
- Data Ingestion and Telemetry
- Intelligent Threat Detection, Research, and Threat Hunting
- Threat and Incident Analysis via Deep Security Analytics
- Advanced Managed Security Operations Center (SOC) Offerings

Managed SOC Services

- » 24/7 monitoring, preventive maintenance threat analysis, threat identification, and response support
- » Integrated modern security frameworks and solutions such as SIEM-SOAR, Advanced Threat Protection
- » Integrated proprietary security platforms such as Cloud4C SHOP (Self-Healing Operations Platform)

Cybersecurity Assessment and Compliance-as-a-Service

- » End-to-end strategic and consultative support at any stage of cybersecurity modernization and strategy development
- » Access to readiness workshops, audits, reporting, vulnerability assessment services, data security management services
- » Fail-proof compliance to local, national and international regulatory standards



Managed Cloud Access Security Broker (CASB)

Our CASB service enables better controls to safeguard cloud security.

- » Uncover shadow and sanctioned IT discovery, providing a consolidated view of your enterprise cloud usage and users who access data from any location
- » Enforce data security policies to prevent unwanted activity based on data classification, discovery, and monitoring user activity
- » Gain adaptive access controls to prevent unwanted devices, users, and applications from accessing your cloud services
- » Ensure compliance with regulations and standards while ensuring accountability for cloud usage

Threat Intelligence Solutions

- » Integrated advanced threat intelligence solutions within the organizational security architecture, powered by Microsoft, OSINT, STIX&TAXI, MIS
- » Consolidated deep analytics from multiple sources and bolster risk strategies with advanced insights
- » Improved threat hunting, data forensics, contextual security management capabilities, and more

Extended Detection and Response (XDR)

- » XDR provides accurate, context-rich alerts to security teams. It goes beyond endpoints and analyses data across endpoints, networks, servers, cloud workloads, SIEM and much more
- » Sifts through thousands of information logs by leveraging the power of AI, ML and automation
- » Provides a unified, single pane of glass view across multiple tools and attack vectors
- » We have done out-of-the-box integrations and pre-tuned detection mechanisms across multiple different products and platforms to improve productivity, threat detection and forensics

Cloud Security Monitoring

Security monitoring helps you take full advantage of the cloud and hybrid IT. Actionable intelligence from continuous monitoring provides early warning about anomalies to investigate and resolve versus routine incidents and thereby increasing your security and efficiency. Benefits include:

- » Monitoring across Cloud service platforms such as AWS, Microsoft Azure, GCP and Microsoft Office 365 while reducing monitoring complexity
- » Protect critical applications and data
- » Improve your efficiency by leveraged elite threat intelligence
- » Maintain compliance

DevSecOps

- » Integrated security solutions and frameworks as part of the development lifecycles and not as perimeter strategies
- » Address DevOps security objectives, SAST/DAST Security, Integration Testing, CI/CD Security, DevOps Security Orchestration, Vulnerability Analysis, etc.

Dark Web Monitoring and Protection

Intelligent Dark Web Scanning to detect the presence of org data, monitor the Dark Web end-to-end for lurking threats and protect databases using preventive solutions.

Asset Security

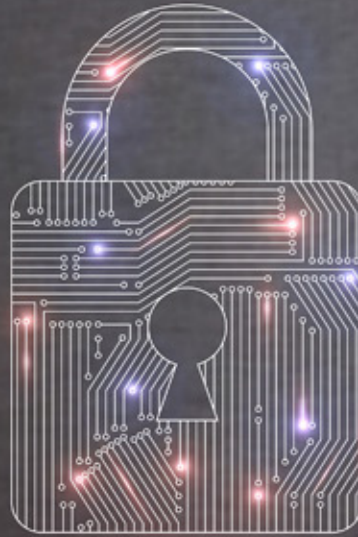
- » Monitor, analyze, and respond to threats with un inching ease and deep threat intelligence across the IT stack
- » Integrated advanced security platforms and automation solutions such as cloud-native tools, SIEM-SOAR, and more

Integrated Security Offerings from Cloud4C and Microsoft

Cloud4C has partnered with Microsoft to offer security services consisting of Azure Sentinel, Azure Information Protection, Microsoft Defender Advanced Threat Protection, Azure Active Directory (AD), Microsoft Intune and more.

We leverage Microsoft's leading technology platforms to provide robust incident response and managed security services.

With Microsoft Security Center of Excellence at Cloud4C, we offer next-gen integrated security solutions to provide 24x7 cyber defenses for protecting every enterprise asset. Cloud4C's comprehensive Next-Gen SOC services include Managed SIEM, EDR, analytics, threat hunting, threat intelligence, SecOps, and SOAR services.



Azure Sentinel Deployment

-  Perform assessment of existing infra, gather requirements, provide upfront cost estimate, and more
-  Deploy and configure initial Azure Sentinel
-  Review devices and log types, both for on-premises and in the cloud and decide which ones to move to the cloud
-  Assist with the log onboarding activities
-  Create alerts and playbooks
-  Alerts tune-up

Azure Sentinel Management

-  Continuous re-tuning of existing alerts, playbooks and creating organization specific use cases
-  Monitoring and availability of all log sources (cloud or on-premises)
-  Regular alerts and monitoring of cloud SIEM costs
-  Periodical service review depending upon the customer ask
-  Custom dashboards with relevant customer information
-  Threat Intelligence open source feeds integration

About Cloud4C

Cloud4C is the world's largest Application-focused and Automation-driven cloud managed services provider in high-growth economies and fast-growing sectors, serving 4000+ enterprises including 60 of the Fortune 500 multinationals in 25 countries spread across the Americas, Europe, Middle East, APAC. Equipped with 25 Centers of Excellence, 2000+ skilled and certified cloud experts, comprehensive cloud security framework comprising 40+ security controls, pre-met compliances with leading industry regulations, Cloud4C helps in managing mission-critical workloads across hybrid and multi-cloud environments and successfully delivered cumulative uptime of 99.95% for complex enterprise applications such as ERP, CRM, BI & BW, Core Banking, etc.