

G-Cloud 15

Service Definition for Managed Cyber Services



Table of Contents

About Us	3
Our Mission	3
Security Operations Centre (SOC) & SOC as a service	4
Summary	4
Features	4
Benefits	5
Managed SIEM Service	7
Summary	7
Features	7
Benefits	8
Vulnerability Management Service	9
Summary	9
Features	9
Benefits	10
Security Awareness Training	10
Summary	10
Features	11
Benefits	12
Managed Detection and Response (MDR)	12
Summary	13
Features	13
Benefits	14
Dark Web Monitoring	14
Summary	15
Features	15
Benefits	15
Continuous Pentesting	17
Summary	17
Features	17
Benefits	18
User Awareness Training	19
Summary	19
Features	19
Benefits	19
Third Party Supplier Assurance (VRM)	21

Summary	21
Features	21
Phishing Testing	23
Summary	23
Features	23
Benefits	23
Pen Testing	24
Summary	24
Features	24
Benefits	25
CrowdStrike 24x7 Falcon Identity	26
Summary	26
Features	26
Benefits	27
CrowdStrike Falcon Cloud Security	28
Summary	28
Features	28Pen

About Us

Mondas is a cyber security consultancy that provides advanced threat protection services: we can minimise your cyber risk, protect your privacy, and ensure compliance so you can focus on what you do best.

Whether you need to overhaul your security processes and technologies or have a specific project that needs support, we can deliver on time and budget.

We are accredited with the following certifications:



Our Mission

Our mission is simple: We want to provide the same high-end security service that large corporations have been benefiting from for years, but at a price point that opens up the market to a much larger audience. By combining our expertise in planning and design with modern cloud-based technologies and a team of talented information security professionals, we have created a range of services that does exactly that.

Service

Security Operations Centre (SOC) & SOC as a service

Summary

Our SOC team supports operations throughout the entire incident response lifecycle. Before undergoing remediation, the threat must first be detected, investigated, and responded to. Depending on your business preference, our analysts can remediate these threats for you.

Once an alarm is detected that requires attention, our SOC team will follow agreed-upon playbooks to remediate and contain the threat. This may be to isolate a machine from the network or roll back systems to a safe state at any time of the day or night. No input is necessary from our customers, and a follow-up report summarising the incident will be sent.

Features

SIEM and Log Management: Our extensive reporting systems gives organisations the ability to correlate, analyse, and securely store any event data from the entirety of their network.

Asset Discovery: Our comprehensive solution will scan an organisation's network and provide unique reports to show exactly who and what is connected to their environment.

Vulnerability Management: Mondas' in-depth Vulnerability Management tools allow organisations to identify, classify and mitigate any cyber threats to their assets across their entire network.

Intrusion Detection: Our dedicated Intrusion Detection and Response tool provides organisations with built-in host, network, and cloud intrusion detection technologies to detect and respond to threats faster.

Endpoint Detection and Response: Our extensive EDR security solution will continuously monitor your organisation's endpoints in the cloud and on-premise. This will detect any threats or changes to critical files, giving you greater peace of mind.

Behavioural Monitoring: Mondas' User Behavioural Analytics (UBA) allows organisations to track actors and assets within their environments. This will identify and alert them to suspicious behaviour, user activities, or compromised systems.

Dark Web Monitoring: We check your corporate identity, employee, user, and customer credentials against the largest breached datasets to identify stolen passwords before cybercriminals can use them.

Security and Compliance Reporting: Mondas' system provides purpose-built, customisable reports that meet regulation standards and compliance frameworks

Benefits

Dedicated team of security experts: Your business will benefit from the guidance and expertise of a dedicated security team.

Efficient Resource Allocation: You will be able to focus solely on supporting your business operations while we protect you from threats.

Reduction of risk: Our Managed SOC combines our various services to provide a comprehensive cyber security coverage. Our analysts can detect and respond to even the most advanced threats.

Rapid threat detection and response: Our analysts will monitor your environment 24x7x365, so any threats to your business will be detected and remediated in real-time.

Cost effective: Our Managed SOC service combines our most popular services into one cost effective package, and offers an attractive alternative to managing cyber threats internally.

Improves cyber insurance coverage eligibility: Our Managed SOC service improves cyber insurance coverage eligibility by mitigating business risks and guaranteeing continuous threat detection.

Secure remote working environments: Our Managed SOC service effectively ensures that your networks remain secure regardless of remote working environments.

Proactive mitigations; Our SOC team leverages the knowledge they gain from monitoring suspicious activities to produce policies and strategies that help prevent future attacks.

Service

Managed SIEM Service

Summary

Mondas' managed SIEM will enhance your business' cyber security posture by giving you 24x7x365 security monitoring and alerting capabilities across your entire organisation, and centralising all logs within a single pane of glass view.

Our managed SIEM service ensures a scalable SIEM platform which will be continuously fine tuned to specific use cases in order to ensure effective management and maintenance of the SIEM.

Features

Real-Time Threat Detection: We will identify potential security threats in real-time, using advanced analytics and tailored correlation rules. These will ensure we respond quickly to minimise the impact of any security incidents.

Incident Response and Remediation: Mondas will forensically investigate security alerts that are generated within the SIEM to determine its source. We will then provide remediation advice and guidance to mitigate any issues that have been highlighted.

Integrated Threat Intelligence: Our managed SIEM incorporates all the leading threat intelligence feeds, in order to enrich and validate the latest emerging threats across the cyber landscape. This will give you proactive defensive capabilities.

Customised Alerts and Notifications: We work with our customers to ensure alerts and rules are customised to suit your businesses risk tolerance and operational requirements. This will keep false positives at a minimum, and focus on providing notifications for real threats within your environment.

Benefits

Fast Deployment: SIEM solutions can be deployed and configured into your IT environment within hours, with no effect on your normal operations.

Complete Visibility: SIEM solutions will centralise all logs generated from your security tools within your entire IT environment into one single pane view, giving you complete visibility.

Dedicated Team of Security Experts: You will benefit from the expertise of a dedicated team of security professionals who are experienced in a wide range of domains.

Reduction of Risk: Having a managed SIEM to monitor your IT environment around the clock will substantially reduce the risk of your business falling victim to a cyber attack.

Cost Savings: Outsourcing your SIEM solution to a specialist provider will reduce the expense required to hire, train and retain an in-house information security team.

Efficient Resource Allocation: With a team of experts managing your threat environment, your personnel will be able to focus on ongoing business initiatives.

Service

Vulnerability Management Service

Summary

Mondas' vulnerability management programme is tailored to your organisation, and will keep your network safe from internal and external vulnerabilities. Utilising our highly skilled experts who work with the latest vulnerability scanning tools allows you to prioritise and manage your cyber risks, quality and compliance.

Features

Identify: Identify, discover, and target each asset that will be included within the vulnerability assessment.

Prioritise: Once each asset has been discovered, agree and assign a value to each one, which will be based upon its impact or criticality to your business.

Assess: Based on the assets that we have discovered, our team will conduct comprehensive scans using Tenable to provide a high fidelity view of your risk. We will create executive reports to ensure that all assets have been scanned properly, and provide us with results.

Remediate: After reviewing the vulnerability reports, we will agree on a strategy for remediating the identified vulnerabilities, or in some cases accept the risk posed by a vulnerability.

Reassess: Once the vulnerabilities have been remediated, we will ensure that all threats have been eliminated. This will show that the mitigation strategies we implemented are working.

Improve: Our team will then look for ways to improve and further protect your network against the latest threats. We will continuously review the vulnerability management process to ensure that it is driving maximum value.

Benefits

Regular Reporting and Remediation: Running regular vulnerability scans will ensure that any vulnerabilities across your systems are identified before they become a real security risk.

Understand Your Threat Landscape: Regular scans will provide you with a well rounded view of your business' threat landscape and the vulnerabilities your company is exposed to.

Monitor Potential Vulnerabilities: Vulnerability scans can be scheduled to fall in line with technical changes or new releases to ensure no vulnerabilities slip through the net.

Meet Compliance Requirements: Running vulnerability scans will help your business meet regulatory and industry standards by identifying, prioritising and remediating any vulnerabilities.

Targeted Scanning and Reporting: We target our scans and reporting capabilities on specific infrastructure areas including internal, external, databases, web applications or firewalls.

Efficient Resource Allocation: With our team of experts managing your vulnerabilities, your personnel will be able to focus on ongoing business initiatives.

Service

Security Awareness Training

Summary

Mondas' security awareness training will help protect your data, systems, and networks from cyber threats and improve overall security awareness throughout your organisation. It will educate your employees on identifying potential threats and how to respond to them appropriately.

Regular simulated exercises will showcase how your business would perform against real-world threats, and additional training can be provided and tailored to specific teams or users to improve their security awareness.

Features

Complete a baseline test: Generate your business' benchmark score by completing an initial assessment before any training. This will help us understand the risk for both individuals and your business. The results of this exercise will create a baseline score and shape our training strategy.

Educate your users: Once a baseline score has been generated, we will allocate tailored training content to your business across various mediums. Scheduled reminders will be sent to employees to support their upskilling and improvement of threat awareness.

Re-test your users: After completing their training content on potential threats, a simulated exercise will be sent to retest your users. Your benchmark scores and tailored reporting will show any trends and improvements the training has made to your organisation's score.

Analyse the results: We leverage AI to analyse your users' unique data and attributes and compare it against all historical data of our users to generate relevant security training for an individual based on their skill level. Reports tailored to your organisation's unique needs and goals will provide detailed insights into your business' security posture. This will allow you to make informed, data-driven decisions for your long-term security strategy.

Allocate tailored training: Specific training content will be pushed to specific teams or individuals in line with the wider security strategy. This will be tailored to their security knowledge and preferred mediums of working to maximise outcomes.

Benefits

Reduces human error: Once trained to identify and respond to security threats, your employees are less likely to make security mistakes.

Protects sensitive information: Security awareness training will help your organisation ensure that your employees don't negligently lose any sensitive data.

Increases security awareness: Security awareness training helps employees identify potential cyber attacks, such as phishing, ransomware, malware, and social engineering.

Reduces risks: Training your employees to identify threats reduces your organisation's risk of falling victim to a successful cyber attack.

Bolsters your security measures: Security awareness training adds an extra layer of protection for your organisation by reinforcing good cyber hygiene practices.

Maintains customer trust: Security awareness training can help maintain customer trust by demonstrating your organisation's commitment to data protection.

Service

Managed Detection and Response (MDR)

Summary

Mondas' Managed detection and response (MDR) provides comprehensive threat detection and prevention for your business. We will onboard your existing solution or recommend a solution that best meets your requirements. If any threats circumvent your security perimeter, our team will detect, investigate, and remediate them. This service ensures that your business is well-equipped to effectively manage and mitigate any targeted cyberattacks on your endpoints.

Features

Detection: Mondas' MDR service leverages the ability of specialised software and skilled security analysts to prevent and detect security breaches proactively. This involves cloud threat monitoring, vulnerability scanning, and log data collection across your business' endpoints.

Threat Hunting: Our analysts engage in proactive threat hunting to detect even the most advanced and imperceptible threats. This process allows them to create new threat intelligence and identify new markers of cyberattacks.

Analysis: If any patterns or irregularities indicate the presence of a threat are identified, our analysts will investigate the issue. All security incidents will be subject to comprehensive analysis to determine the root cause of the breach.

Remediation: Our MDR service combines manual and automated response capabilities to ensure our analysts can quickly prevent or redress any detected threats across your endpoints.

Reports: Our team will produce regular threat and compliance reports to ensure you have complete visibility of the threats our analysts protect your business against and the measures they take to do this.

Benefits

Dedicated team of security experts: Your business will benefit from the guidance and expertise of a dedicated security team.

Efficient resource allocation: You will be able to focus solely on supporting your business operations while we focus on protecting you from threats.

Reduction of risk: Our analysts protect against a wide range of advanced attacks. They can detect and respond to even the most complex threats before they impact your business.

Rapid threat detection and response: Our analysts will monitor your environment 24x7x365, so any threats to your business will be detected and remediated in real-time.

Cost effective: Our MDR service is a cost effective alternative to managing cyber threats internally, which is expensive, laborious, and often inadequate.

Improves cyber insurance coverage eligibility: Our MDR service improves cyber insurance coverage eligibility by mitigating business risks, and guaranteeing continuous threat detection.

Service

Dark Web Monitoring

Summary

Hunt the dark web to uncover personal or business information available on the dark web. Mondas uses AI, Machine Learning, and human interactions to monitor the Deep and Dark Web automatically. Alerts will be triggered if your corporate identity, employee, user, or customer credentials are flagged against breached datasets of personal information, passwords, and credentials.

Features

Regular Security Checks Our service will continuously scan the dark web for sensitive information being sold or shared there. This will ensure that we can identify any data breaches so you can take swift action to minimise their impacts on your business.

Real time breach alerts: Our team will notify you when your sensitive information is found on the dark web. We will provide details on how long the data has been exposed and the methods used to gain access. Alerts are generated in real-time and within seconds of a security breach being evidenced.

Enhanced Threat Intelligence: Mondas will provide you with the early detection of leaked data, insights into insider threats, and the context behind any cyber breaches. This information can be leveraged to enhance your threat intelligence.

Monthly Executive Reports: Our team will create monthly reports summarising our findings. These reports will include contextual information for all security breaches, including your exact stolen credentials and intellectual properties. This will help you mitigate your risks moving forward.

Benefits

Safeguard Employee and Client Data: Dark web monitoring will help you identify any sensitive data that has been breached and prevent cybercriminals from using it.

Discover Data Breaches Quicker: Continuous dark web monitoring will inform you of any stolen or leaked company data in real-time.

Continuous Monitoring Our dark web monitoring service continuously searches the dark web and monitors millions of sites in real-time.

Manage Your Brand Reputation: Detecting data breaches across the dark web in real-time will allow you the time to mitigate any reputational damage you may face.

Improved Detection and Response Capabilities: The dark web can be a blind spot for many businesses. Monitoring it will allow you to remediate cyberattacks at the earliest stage.

Better Prepare for Future Attacks: Understanding the context behind previous breaches will help us form a vigorous action plan to prevent future attacks.

Service Pen Testing

Summary

Mondas' penetration testing service provides a rigorous, expert led evaluation of your organisation's security posture. Our CREST and CHECK certified service includes targeted technical assessments to simulate real world attacks, allowing you to identify and remediate vulnerabilities before they can be exploited.

Every engagement is tailored to your specific infrastructure, resulting in a technical report that provides clear remediation advice.

Features

Comprehensive Infrastructure Testing: We conduct deep dive assessments of your internal and external network infrastructure to identify misconfigurations and architectural flaws.

Web Application and API Assessment: Our testers perform targeted security reviews of your web applications and interfaces, testing for common vulnerabilities.

Endpoint and Asset Security Reviews: We offer specialised testing for endpoints, including "stolen laptop" scenarios for example, to ensure that data remains protected even if hardware falls into the wrong hands.

Red Team Attack Simulations: We can provide Red Team exercises designed to test your detection and response capabilities against sophisticated, multi-stage attack patterns.

Concise Technical Reporting: Every test concludes with a high quality report that translates complex technical findings into actionable business risks and clear remediation steps.

Benefits

Stakeholder Assurance: Provides objective, third party validation that your security controls are effective and that sensitive stakeholder data is adequately protected.

Alignment with Global Standards: Ensures your technical testing meets the requirements of rigorous compliance frameworks such as ISO 27001.

Proactive Identification: Reveals hidden security gaps in your systems that automated tools may miss, allowing for targeted remediation of high risk vulnerabilities.

Enhanced Incident Resilience: By addressing the weaknesses exposed during testing, you significantly reduce the likelihood of a successful cyber attack and improve your overall resilience.

Service

Continuous Pentesting

Summary

Continuous penetration testing replaces one-off assessments with ongoing, adaptive security validation. It continuously identifies new vulnerabilities, verifies remediation, supports compliance, and reflects real operational change. This provides stronger assurance, whilst also providing better prioritisation and reduced exposure time.

Features

Continuous Adaptation

Security assessments run continuously against your live environment, adapting automatically to varying environment adaptations such as infrastructure changes, new applications and identity updates. This ensures your security posture is always measured against current reality rather than outdated snapshots, providing far more accurate and actionable insight into your true exposure.

Continuous Validation

Every fix is independently verified through repeat testing, ensuring vulnerabilities are genuinely resolved rather than cosmetically closed. This prevents false confidence, reduces reoccurring findings, and gives technical teams certainty that remediation efforts have permanently removed real attack paths.

Continuous Evidence

Continuous testing automatically generates structured, auditable evidence of ongoing risk management. This supports regulatory requirements, client assurance, and internal governance by demonstrating proactive control monitoring rather than reliance on historic point-in-time assessments.

Continuous Priorisation

Results are delivered in a steady, risk-ranked flow based on real exploitability and business impact. This prevents overwhelming reports, enables efficient decision-making, and ensures

security and IT teams focus effort where it delivers the greatest reduction in organisational risk.

Benefits

Shortens Exposure Duration

Vulnerabilities are discovered and addressed quickly, dramatically reducing the time attackers can exploit weaknesses. This significantly lowers the likelihood of breaches, operational disruption, and reputational damage caused by undetected or long-lived security flaws.

Assurance

You maintain an always-current understanding of your security posture, rather than relying on outdated assessments. This enables leadership, security teams, and stakeholders to make confident, informed decisions based on live risk intelligence.

Faster Remediation

Smaller, continuous findings allow teams to resolve issues rapidly and efficiently. This avoids remediation backlogs, reduces fatigue, and ensures security improvements are implemented while the context and ownership are still clear.

Governance

Continuous penetration testing demonstrates mature, proactive risk management. It strengthens regulatory confidence, and trust by showing that security is treated as an ongoing operational discipline, not a periodic checkbox exercise.

Service

User Awareness Training

Summary

Mondas' User Awareness Training is designed to transform your employees from a potential security risk into your strongest line of defence. By focusing on the human element of cyber security, we provide the knowledge and tools your staff need to protect your organisation and recognise the signs of an attack in their day to day work.

Features

Targeted Learning Pathways: We will work with you to determine the current security maturity of your organisation then deploy personalised learning that aligns with your specific needs. This ensures your employees receive training that is useful and relevant to their day to day work.

Regular Training Campaigns: Our team designs and schedules training cycles that deliver fresh content at regular intervals, ensuring security awareness remains a continuous process rather than a one off event.

KnowBe4 Integration: We can deploy and manage the industry leading KnowBe4 platform to deliver a comprehensive library of security awareness content, including interactive modules, videos, and newsletters.

Benefits

Industry Leading Content: Users benefit from the world's largest library of security awareness training, ensuring the content is always relevant, high quality, and engaging.

Quantifiable Behaviour Change: By tracking users' scores over time, leadership will be able to see tangible evidence of the organisation's improved security posture and reduce likelihood of human error.

Strengthened Security Culture: Continuous engagement fosters a culture where employees will be more knowledgeable. Feel more personally responsible for the safety of the organisation, and be more likely to report suspicious activity.

Service

Third Party Supplier Assurance (VRM)

Summary

The Mondas Third Party Supplier Assurance service is powered by SecurityScorecard and helps you properly manage your vendor risk management. This service actively monitors your third parties to see who is failing to meet their specific target requirements allowing you to initiate prompt communication and identify remediation actions to reduce the risk to your organisation.

Features

Continuous Security Monitoring: Utilising the SecurityScorecard platform, we provide a non-intrusive view of your vendors' security postures, including key risk factors such as DNS Health, IP Reputation, Patching Cadence and more.

Collaborative Remediation Management: Unlike traditional reporting, this service facilitates direct collaboration with vendors. We can act as the intermediary providing vendors with the specific findings, and allowing them to improve their security score.

Evidence Based Validation: When vendors claim to have remediated an issue, our service can validate the fix through rescanning and expert review, ensuring the risk has been truly remediated.

Executive Reporting: The service includes clear grading and risk matrices to translate the technical data into business terms allowing your stakeholders to easily understand your vendors' performance against internal risk appetite thresholds.

Benefits

Risk Reduction: By proactively scanning and promptly informing the vendors, we significantly shorten the time to remediation.

Reduced Internal Resource Drain: Third party risk management is notoriously labour intensive. Our service can handle the heavy lifting from outreach to rescanning.

Strengthened Vendor Trust: This process will help foster a security first culture throughout your supply chain. By helping your vendors to improve their own security, you create a safer business ecosystem that is better protected.

Service

Phishing Testing

Summary

We utilise KnowBe4's platform to deliver realistic simulated phishing attacks (the most common cyber attack vector) that seamlessly integrate with our User Awareness Training service. These fully managed campaigns provide a safe, controlled environment to test and reinforce employee vigilance against sophisticated social engineering threats.

Features

Precision Customization: Mondas designs bespoke campaigns utilising custom templates, specific intervals, and precise timings to accurately reflect the threats your specific industry faces without disrupting daily operations.

AI-Driven Simulation: Leveraging KnowBe4's AI, our testing simulates dynamic, real-world attacks that work in conjunction with training modules in our User Awareness Training service to educate your employees and build phishing resilience.

Benefits

Measurable Risk Reduction: Mondas reports on the results to identify users who are most susceptible to phishing attacks. We use this insight to strengthen your employee's phishing defenses through targeted learning modules which include videos, interactive games, quizzes and more.

Resilient Security Culture: Transform your workforce into a strong "human firewall," ensuring that security awareness remains top-of-mind through consistent, adaptive testing cycles.

Service

CrowdStrike 24x7 Falcon Identity

Summary

This ISO 27001 certified service stops identity based breaches in real time across hybrid environments. Our UK based SecOps team monitors for signs of credential abuse, lateral movement, and privilege escalation on your network to ensure total identity protection.

Features

24x7 CrowdStrike Powered Service: Our SOC team provides continuous, around the clock monitoring of your identity infrastructure using the CrowdStrike platform.

Native Integration: We provide seamless, native integration with both on-premises Active Directory and Entra ID to ensure unified visibility across hybrid estates.

Real Time Detection: Our analysts identify and block unauthorised lateral movement and credential theft as it happens, stopping attackers before things escalate.

AI Powered Analytics: We leverage AI powered analytics to proactively hunt for hidden identity based threats and compromised accounts that traditional tools might miss.

MFA Enforcement: We manage the dynamic enforcement of Multi-Factor Authentication (MFA) based on real time assessments of individual user risk levels.

Benefits

Real Time 24x7 Monitoring: Provides constant surveillance of your most critical security layer by specialised professionals.

Faster Remediation: Significantly reduces the time to contain threats by utilising pre-configured playbooks.

Complete Visibility: Delivers a centralised view of your entire identity risk posture through high fidelity dashboards.

Protect Identities: Ensures that service accounts and machine identities are as secure as your human users across all environments.

Reduce Attack Surface: Improves security by extending modern MFA protection to older, legacy systems that do not natively support it.

Service

CrowdStrike Falcon Cloud Security

Summary

Mondas provides expert led protection for your cloud native environments by leveraging the power of CrowdStrike Falcon Cloud Security for 24x7 Managed Detection and Response (MDR), threat hunting, and incident response. This service will secure your applications and infrastructure across the entire development lifecycle.

Features

Threat Discovery: Utilise CrowdStrike to identify, track, and remediate threats within your cloud and containers.

Image Security: Integrate security directly into your continuous integration and deployment pipelines to identify vulnerabilities before images are deployed.

Zero Day Tracking and Risk Profiling: Native integration to track zero day vulnerabilities and maintain a real time risk profile of your cloud infrastructure.

Multi-Cloud Support: Full support for major public cloud providers (AWS, Azure, GCP) as well as private cloud environments, ensuring a unified protection across hybrid estates.

24x7 Expert Threat Hunting: Direct access to expert threat hunters who proactively search for sophisticated cloud specific attacks.

Benefits

Real Time Detection and Response: Benefit from real time detection and automated response capabilities to stop cloud breaches as they happen.

End to End Visibility: Gain a comprehensive understanding of your vulnerabilities from the initial build stage.

Total Visibility: Achieve complete visibility across your environment, including detection, response, proactive threat hunting, and attack surface reduction.