Crown Commercial Service
Supplier

G-Cloud 15

Digital Forensics & Incident Response Service

Atos

Table of contents

1. What is the Digital Forensics and Incident Response Service? 3
2. What does it deliver? 4
3. What technology does it use? 10
4. What terms apply? 16
5. Termination 17
6. How do I order? 18
7. Glossary 19
8. Why Atos 20

Crown Commercial Service *Supplier*

Atos

1. What is the Digital Forensics and Incident Response Service?

The Digital Forensic and Incident Response (DFIR) for Cybersecurity service from Atos is a comprehensive, enterprise-grade offering that empowers Public Sector organisations to effectively identify, investigate, contain, and remediate security incidents across complex cloud, hybrid, and on-premises environments.

The service is specifically architected to support Public Sector organisations managing diverse IT environments, which typically encompass multiple cloud platforms, on-premises systems, legacy infrastructure, and increasingly, operational technology (OT) environments.

By providing a holistic, integrated approach to incident response and forensics, Atos enables Public Sector organisations to rapidly detect, thoroughly investigate, effectively contain, and successfully recover from security incidents, regardless of their origin or complexity.

The service consists of the following core key components:

- Security Incident Response
- Digital Forensics (remote and on-site)
- Malware Analysis.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

Atos' Digital Forensic and Incident Response (DFIR) service is comprehensive and multifaceted, encompassing a broad spectrum of activities designed to proactively identify, effectively manage, and rapidly mitigate cybersecurity incidents.

DFIR serves as a critical pillar of Public Sector cybersecurity frameworks, focusing on meticulous investigation and accelerated response to critical incidents, including sophisticated cyberattacks, data breaches, ransomware attacks, and other security compromises.

The primary objectives of DFIR are to comprehensively assess incident scope, identify root causes with precision, implement immediate containment strategies, thoroughly eradicate identified threats, and successfully restore affected systems to secure operational states.

Key aspects of the DFIR services

Proactive Incident Detection and Triage:

- Continuously monitoring and proactively identifying potential security incidents using advanced threat detection technologies, machine learning algorithms, and behavioural analytics
- Conducting comprehensive initial triage to assess severity, business impact, and potential cascading effects of identified incidents, enabling optimal prioritisation and resource allocation
- Performing false positive analysis to ensure efficient use of resources and accurate threat identification.

In-Depth Forensic Investigation:

- Meticulously collecting, preserving, and analysing digital evidence using forensically sound methodologies to establish comprehensive incident timelines and determine full attack scope
- Examining artefacts, logs, network traffic, memory dumps, IoCs, and other relevant data sources to identify specific attack vectors, tools, and tactics employed by threat actors
- Conducting advanced memory, disk, and cloud forensics to uncover hidden malicious activities, trace lateral movement, and gather court-admissible evidence
- Identifying Patient Zero and mapping breach extent to understand initial compromise points and full incident scope.

Comprehensive Malware Analysis:

- Performing detailed static and dynamic analysis of malicious software to understand functionality, command-and-control mechanisms, persistence techniques, and potential organisational impact
- Determining the specific purpose and methods used by malware through reverse engineering using commercial and public toolsets
- Developing customised signatures, YARA rules, and Indicators of Compromise (IoCs) based on analysed malware to enhance detection capabilities and prevent incident recurrence
- Providing custom reports detailing the complete composition and behaviour of identified malware.

Swift Incident Containment and Eradication:

- Implementing immediate, surgical containment measures to isolate affected systems, prevent lateral spread, and minimise business disruption while maintaining evidence integrity
- Systematically identifying and removing all malicious artefacts, including backdoors, webshells, malware, persistence mechanisms, and unauthorised access points from compromised systems
- Coordinating with SOC and CSIRT teams to ensure comprehensive threat elimination across the environment.

Comprehensive Post-Incident Reporting:

- Compiling detailed technical reports encompassing forensic findings, attack reconstruction, timeline analysis, containment actions, and strategic recommendations for security enhancement
- Providing executive-level briefings that clearly communicate incident impact, response effectiveness, lessons learned, and risk mitigation strategies to senior stakeholders and board members
- Documenting all findings for potential criminal or regulatory proceedings support.

Legal and Compliance Support:

- Assisting organisations in navigating complex legal and regulatory requirements related to cybersecurity incidents, ensuring compliance with GDPR, NIS2, MCSS, and sector-specific regulations
- Providing well-documented, court-admissible evidence preservation and examination with expert witness testimony to support legal proceedings

- Offering criminal and regulatory proceedings recommendations to guide organisations through legal processes.

Proactive Threat Intelligence Integration:

- Leveraging cutting-edge threat intelligence platforms and feeds to enhance incident detection and response capabilities, maintaining situational awareness of emerging threats
- Conducting threat actor capabilities analysis to understand adversary sophistication and potential impact
- Incorporating actionable intelligence about threat actors, campaigns, and their Tactics, Techniques, and Procedures (TTPs) into incident response strategies, playbooks, and defensive controls.

Robust Incident Response Planning:

- Conducting Incident and Forensic Baseline Workshops to establish organisational readiness
- Developing comprehensive, tested incident response plans that establish clear roles, responsibilities, escalation procedures, and communication protocols for coordinated incident management
- Establishing dedicated communication channels for crisis management and stakeholder coordination
- Regularly updating and exercising incident response plans based on lessons learned, threat landscape evolution, and industry best practices.

Recovery and Restoration Services:

- Providing data recovery and system restoration capabilities to minimise operational disruption
- Implementing preventative measures and security enhancements based on incident findings
- Delivering extended post-incident services to ensure complete recovery and improved resilience
- Offering incident recovery recommendations and consultation throughout the restoration process.

Continuous Improvement and Resilience:

- Conducting thorough post-incident reviews, root cause analyses, and tabletop exercises to identify improvement opportunities
- Implementing lessons learned and industry best practices to enhance organisational cybersecurity resilience continuously
- Providing ongoing consultation to strengthen security controls and reduce the likelihood of future incidents.

DFIR Service Modules

Atos' DFIR service is delivered through comprehensive, modular offerings that can be tailored to specific organisational requirements:

Cyber Security Incident Response Modules:

- Incident Baseline Workshop
- Artefact & Malware Analysis
- Post-Incident Report & Recommendations
- Establish Communications Channels
- Threat Actor Capabilities Analysis
- 24x7 CSIRT Support
- False Positive Analysis
- Breach Extent Identification
- Additional CSIRT Hours
- Incident Analysis
- Incident Recovery Recommendations/Consultation
- Incident Containment
- Patient Zero Identification
- Incident Eradication
- Criminal/Regulator Proceedings Recommendation.

Digital Forensics Modules:

- Forensic Baseline Workshop
- Criminal Proceedings Recommendations
- Evidence Acquisition

- Evidence Preservation & Examination
- Forensic Report and Workshop.

Cyber Recovery Modules:

- Data Recovery
- System Restoration
- Communications and Reporting
- Preventative Measures & Security Enhancements
- Extended Post-Incident Services.

Service Delivery and Extra Effort Model

DFIR is committed to delivering service within agreed specifications and service levels. For situations requiring additional support:

- Any additional effort exceeding the agreed scope or package hours is evaluated by DFIR management based on available resources and expertise
- DFIR reserves the right to decline support if resources are unavailable or requests fall outside the defined scope of DFIR delivery
- When DFIR involvement is required beyond the agreed package, each extra hour is charged at a fixed rate determined by the DFIR Service Manager
- This ensures transparent pricing while maintaining service quality and resource availability.

Key Service Benefits to Public Sector organisations

Regarding Public Sector organisations, the Digital Forensics and Incident Response service for Cybersecurity delivers critical benefits to the organisation and its stakeholders:

National Security - Safeguarding critical national infrastructure, protecting classified systems, and ensuring the continuous operation of essential government functions across defence, intelligence, and public services.

Public Trust and Confidence - Robust incident response capabilities are essential for maintaining citizen trust and demonstrating the Public Sector's commitment to protecting personal data, democratic processes, and public services.

Compliance with Government Regulations - Helping Public Sector organisations meet stringent regulatory requirements and align with best practices for incident management, including the Minimum Cyber Security Standard (MCSS), National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF), and Government Functional Standard GovS 007.

Protecting Sensitive Information - Defending against unauthorised access, exfiltration, or compromise while maintaining rapid response capability for incidents affecting classified documents, citizen data, health records, and intellectual property.

Collaboration and Information Sharing - Providing structured frameworks for coordinated incident response, threat intelligence sharing, and joint investigations between Public Sector organisations, supporting national cyber defence initiatives.

Skill Development and Capacity Building - Delivering opportunities for Public Sector personnel to develop specialised expertise in incident response, forensic analysis, threat hunting, and emerging security technologies to address evolving threats.

Resilience and Business Continuity - Supporting Public Sector agencies in developing, testing, and implementing effective incident response plans through regular exercises and simulations, continuously improving detection, response, and recovery capabilities to ensure critical service continuity.

Cost Effectiveness - Outsourcing DFIR services to specialised providers offers superior value compared to maintaining full-time in-house incident response teams, particularly considering continuous training requirements, tooling investments, and infrastructure costs

Crown Commercial Service Supplier

Atos

3. What technology does it use?

Atos' DFIR service is delivered through a sophisticated multi-layered approach that combines expert personnel, cutting-edge technologies, and battle-tested processes to provide Public Sector organisations with comprehensive incident response and digital forensics capabilities.

The service delivery model is designed for maximum flexibility and scalability, enabling Atos to meet diverse organisational requirements and adapt to evolving threat landscapes.

The key components of Atos' DFIR service delivery include:

Dedicated Incident Response Team:

- Atos assigns each organisation a dedicated team of certified incident responders, digital forensics experts, and threat intelligence analysts
- The specialised team manages all incident response phases from initial detection through post-incident improvement, maintaining deep familiarity with the organisation's environment
- The team operates 24/7/365 with guaranteed SLAs to ensure rapid mobilisation for critical incidents
- Security Incident Managers are assigned for P1 and P2 incidents to ensure proper coordination and escalation.

Remote and On-Site Support:

- Atos provides seamless remote and on-site support capabilities, with deployment models optimised for incident severity and complexity
- Remote forensics investigation enables immediate evidence gathering and examination of malware, IoCs, logs, and other digital artefacts
- On-site support is available for complex incidents requiring physical evidence collection, air-gapped systems, or situations demanding hands-on intervention.

State-of-the-Art Technology Stack:

- Atos leverages an integrated suite of industry-leading technologies and proprietary tools to deliver effective DFIR services
- This includes next-generation Endpoint Detection and Response (EDR) platforms, advanced SIEM/SOAR systems, cloud-native forensic tools, and real-time threat intelligence platforms
- Forensic analysis tools enable comprehensive examination of digital devices and recovery of critical evidence
- These technologies enable Atos to rapidly detect, investigate, and contain sophisticated security incidents across diverse IT/OT environments.

Standardised Incident Response Processes:

- Atos follows rigorously standardised incident response processes aligned with industry frameworks, including MCSS, NCSC CAF, NIST Cybersecurity Framework, ISO 27035, and SANS Incident Response Methodology
- These proven processes ensure consistent, repeatable, and auditable incident response from initial detection through recovery and lessons learned
- Processes are customised to each organisation's specific requirements, risk tolerance, and operational constraints while maintaining best practice alignment.

Continuous Communication and Reporting:

- Throughout incident response and forensics engagements, Atos maintains transparent, continuous communication with designated stakeholders and crisis management teams
- Regular status updates, investigative findings, and actionable recommendations are provided through secure channels to maintain situational awareness
- Comprehensive incident reports and detailed forensic analyses are delivered with complete documentation of timeline, impact assessment, and remediation actions.

Integration with Existing Security Infrastructure:

- Atos' DFIR service is architected for seamless integration with existing security infrastructure, tools, and operational processes
- This includes native integration with organisational SIEM, EDR, SOAR, ticketing systems, and threat intelligence platforms to ensure unified response capabilities
- Atos collaborates closely with internal security teams to ensure effective coordination, knowledge transfer, and capability enhancement.

Flexible Engagement Models:

- Atos offers adaptable engagement models tailored to specific organisational needs, risk profiles, and budgetary constraints

- Subscription-based models provide continuous incident response coverage with defined SLAs, guaranteed response times, and predictable costs
- Hybrid models strategically combine proactive services—including threat hunting, purple teaming, and tabletop exercises—with reactive incident response support
- Ad-hoc emergency support remains available for immediate crisis response, with rapid deployment of Atos' expert incident response team.

Continuous Improvement and Knowledge Transfer:

- Atos maintains an unwavering commitment to continuous improvement and knowledge transfer throughout service delivery
- Structured post-incident reviews and lessons learned workshops identify enhancement opportunities in both service delivery and organisational security posture
- Atos provides targeted recommendations and strategic guidance to strengthen incident response capabilities, security controls, and cyber maturity
- Dedicated knowledge transfer sessions and hands-on training develop internal team capabilities, ensuring sustainable security improvements.

By delivering DFIR services through this comprehensive, integrated approach, Atos ensures organisations receive expert support, advanced technology, and proven methodologies required for effective cybersecurity incident management. The combination of certified security experts, cutting-edge tools, and battle-tested processes enables Atos to deliver premium services that minimise incident impact, maintain operational resilience, and continuously strengthen security posture.

Benefits

The Digital Forensic and Incident Response (DFIR) service offers a comprehensive suite of benefits that significantly enhance a public sectors organisation's cybersecurity posture and enable effective response to security incidents.

The key advantages include:

- **Proactive Threat Detection** - DFIR services employ advanced tools and techniques to detect security incidents in their early stages proactively. This allows organisations to identify and respond to threats before they escalate, minimising the potential impact on systems and data
- **Minimised Operational Disruption** - By rapidly identifying and containing security incidents, DFIR services play a crucial role in minimising downtime and ensuring business continuity. Swift response and remediation measures prevent prolonged disruptions to critical operations, safeguarding productivity and customer satisfaction

- **Mitigation of Data Breach Impact** - DFIR services enable organisations to contain and mitigate the impact of data breaches swiftly. Through rapid response and containment, the potential loss of sensitive data, intellectual property, and other valuable assets can be significantly reduced, protecting the organisation's competitive advantage and reputation
- **Comprehensive Forensic Analysis** - DFIR services employ advanced forensic analysis techniques to uncover the full scope of a security incident. By determining the attacker's identity, methods, and motives, organisations gain valuable insights to strengthen their security posture and pursue legal recourse if necessary
- **Regulatory Compliance Assurance** - DFIR services assist organisations in meeting stringent legal and regulatory compliance requirements. By providing detailed evidence and documentation of security incidents, DFIR helps demonstrate due diligence and adherence to industry standards, thereby mitigating the risk of legal repercussions and financial penalties
- **Proactive Threat Intelligence Integration** - DFIR services seamlessly integrate real-time threat intelligence feeds, enabling organisations to stay ahead of emerging threats. By leveraging up-to-date threat data, DFIR teams can proactively identify and respond to potential incidents, strengthening the organisation's overall security posture
- **Optimised Incident Response Strategies** - Through meticulous analysis of past incidents, DFIR services provide valuable insights for refining and optimising incident response plans. By identifying areas for improvement and implementing best practices, organisations can ensure a more efficient, coordinated, and effective response to future incidents
- **Heightened Security Awareness** - DFIR services foster a culture of heightened security awareness within the organisation. By sharing lessons learned from incidents and providing targeted training, DFIR helps employees and stakeholders become more vigilant and proactive in identifying and reporting potential security threats
- **Proactive Risk Mitigation** - DFIR services are vital in identifying vulnerabilities and weaknesses in an organisation's security infrastructure. By conducting thorough assessments and providing recommendations, DFIR enables organisations to implement proactive measures to mitigate risks and prevent future incidents
- **Continuous Security Improvement** - DFIR services facilitate regular reviews and assessments of incident response processes and procedures. By identifying areas for improvement and implementing best practices, organisations can continuously enhance their overall cybersecurity posture and stay ahead of evolving threats

- **Reputational Safeguarding** - Effective incident response, facilitated by DFIR services, helps organisations protect their reputation in the face of security breaches. By demonstrating a proactive and robust approach to addressing security incidents, organisations can maintain stakeholder trust and minimise reputational damage from cyberattacks.
- **Resilient Business Operations** - DFIR services build resilience into an organisation's business operations. By minimising the impact of security incidents on critical systems and processes, DFIR helps ensure the continuity of essential functions, even in the face of adverse cyber events.

Licensing Models

Digital Forensic and Incident Response (DFIR) services, there are three primary licensing options available:

Table 1 : DFIR Licensing Models

Summary	Service
Retainer	• A dedicated DFIR team is on standby. • Guaranteed response times. • Proactive threat hunting and monitoring. • Regular reporting and status updates.
Pre-Paid	• Predefined number of DFIR hours or incidents. • Flexibility in resource allocation. • Discounted rates compared to ad-hoc. • Unused hours can be rolled over or refunded.
Ad-hoc	• Pay-per-incident or on an hourly basis. • No long-term commitment. • Suitable for infrequent or unpredictable needs. • Higher rates compared to retainer or pre-paid.

The choice of licensing model can significantly impact the cost and delivery of DFIR services, as each option comes with its own set of considerations and benefits.
When considering the licensing options, assessing the organisation's specific needs, risk profile, and budget is crucial.

- **Retainer** model offers the highest level of readiness and guaranteed response times, making it ideal for organisations with critical assets and a high risk of incidents.
- **Pre-paid** options balance cost effectiveness and flexibility, allowing organisations to purchase a set number of hours or incidents in advance.
- **Ad-hoc** services, on the other hand, are best suited for organisations with infrequent or unpredictable DFIR needs, as they allow for pay-per-incident or hourly engagements without long-term commitments.

Table 2 : DFIR Service Scope

Summary	Retainer	Pre-Paid	Ad-Hoc
Scope	Digital Forensics Incident Response Malware Analysis	Digital Forensics Incident Response Malware Analysis	Digital Forensics Incident Response Malware Analysis
Support is guaranteed	Yes	Yes	No
24/7 Incident response readiness P1, P2* security incidents	Yes	Yes	No
24/7 Technical support for high-priority security incidents (P1, P2) *	Yes	Yes	Yes (If the case is approved by CSIRT Management)
10/5 Support for medium and low priority security incidents (P3, P4) *	Yes	Yes	No
Onboarding (preparation phase)	Yes (Full)	Yes (Basic)	No
Financial Model	Fixed monthly payment Optional T&M payment	One-Time Cost (OTC) payment in advance T&M payment per hour above the purchased package	Initial Engagement Fee T&M payment per hour - high tariff
Roll over unused hours to next month(s)	Yes	No	No
Proactive Readiness Activities	Yes	No	No
Platforms (EDR, Forensics, and other tools) for P1 Incident Response and Crisis Management.	Yes (free 30 days)	Yes (free 30 days)	Yes (free 30 days)
Security Incident Manager for P1, P2 incident	Yes	Yes	Yes
Cyber Security Delivery Manager	Yes	No	No

Crown Commercial Service *Supplier*

Atos

4. What terms apply?

To the fullest extent permitted under G-Cloud 15 Framework Agreement and the Call-Off Contract, Atos will provide the Services in accordance with the Atos Supplier Terms (which will include, but may not be limited to , the Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLAs and Supplier Licence Terms and any applicable Third-Party Terms outlined in this Service Description document and the Order Form) and this Service Description document.

For clarity:

- Atos Supplier Terms may be modified in accordance with the provisions of the Call-Off Contract, and remain effective except where expressly overridden.
- Hyperlinks included in the Atos Supplier Terms and Service Description document remain effective where they point to Atos' or the relevant Third-Party Terms or documents. Should a hyperlink cease to function, Atos will work with the client to update it through the agreed procedure.

Crown Commercial Service *Supplier*

Atos

5. Termination

Termination shall be in accordance with:

- The G-Cloud 15 Framework terms and conditions
- Any terms agreed within the Order Form of the relevant Call-Off Contract
- For this specific service, by default Atos ask for at least thirty (30) days prior written notice of termination without cause.

Atos commits to the continued provision of services for the duration of the Call-Off Contract subject to the terms and conditions of the G-Cloud 15 Framework Agreement, the Call-Off Contract, the Atos Supplier Terms and the applicable Third Party Agreements (as defined in the Atos Supplier Terms and indicated in the Order Form) related thereto.

Crown Commercial Service *Supplier*

Atos

6. How do I order?

Please contact our team at: gcloud@atos.net

- We will prepare a quotation for your review, including any applicable volume discounts.
- Once the quotation is agreed, we will issue the necessary documentation (as required by the G-Cloud Framework) and request a purchase order from you.
- Upon receipt of your purchase order, we will configure the services in line with the agreed requirements. Where applicable, you will also receive access to our self-service portal to begin provisioning services.
- If you are a new customer, you may need to complete additional 'new supplier' forms.
- Invoices will be issued to you and to Crown Commercial Service (CCS), quoting the purchase order number, for the services procured.
- We will also submit the required monthly management information reports to Government Procurement.

Crown Commercial Service *Supplier*

Atos

7. Glossary

Term	Definition
CAF	Cyber Assessment Framework
CSIRT	Computer Security Incident Response Team.
DFIR	Digital Forensic & Incident Response
EDR	Endpoint Detection and Response
IOC	Indicators of Compromise
IT	Information Technology
MCSS	Minimum Cyber Security Standard
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
SANS	SysAdmin, Audit, Network and Security
SIEM	Security Information and Event Management
SOC	Security Operation Centre
T&M	Time and Materials
TTP	Tactics, Techniques and Procedures

Crown Commercial Service *Supplier*

Atos

8. Why Atos

Atos has been a trusted partner on every G-Cloud iteration since the framework began, helping Public Sector organisations modernise with confidence. We combine global expertise with deep UK experience, delivering secure, scalable cloud solutions that meet the highest government standards.

As Europe's leading provider of cloud and cybersecurity services, Atos offers end-to-end capabilities - from migration and hosting to SaaS and consultancy - supported by UK delivery centres and strategic partnerships with hyperscalers.

Our focus on innovation, sustainability, and social value ensures that customers not only achieve operational excellence but also contribute to a greener, fairer future. With Atos, you gain a proven partner committed to driving efficiency, resilience, and transformation across public service.

About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net

Atos is a registered trademark of Atos SE. © 2024 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

105043-RR