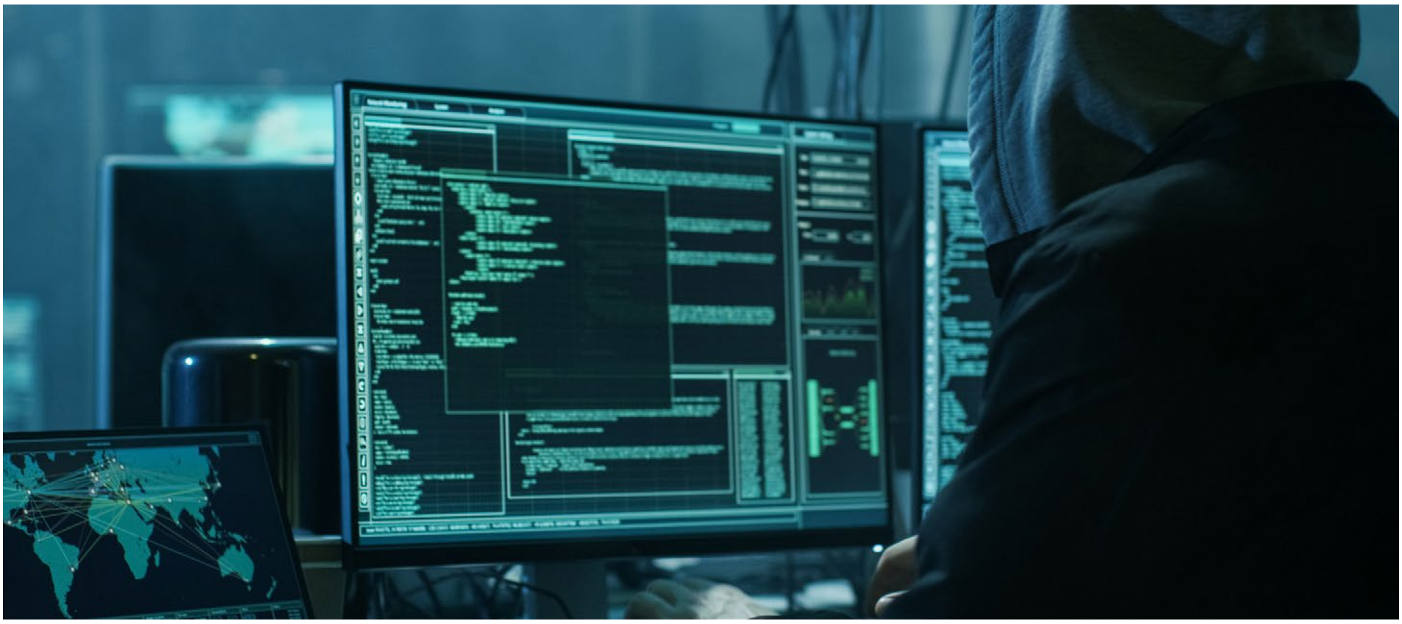
opentext™

SERVICE OVERVIEW

Digital Forensics & Incident Response (DFIR)

Detect, investigate, respond and remediate threats with speed and efficiency with OpenText Cybersecurity Service



Benefits

- **Response to incidents** within minutes
- **Detect threats** across networks, endpoints and cloud
- **Investigation** using AI, ML and NexGen Technology

Industry statistics over the years show a growing skills gap and difficulty for organizations to access DFIR talent. Many believe there is a shortage of cybersecurity skills in their company and the challenge still seems more potent for mid-market and large enterprise businesses. Today, organizations are still struggling to source cybersecurity talent with no material improvement around time-to-hire.

With Digital Forensic investigative experience reaching back as far as 20 years, the OpenText Cybersecurity Services team are professional forensic investigators using the OpenText security solutions stack and best in breed technologies. OpenText DFIR services combined with an Incident Response Retainer are a proactive approach to cyber security and gives organizations the ability to minimize the impact of an incident.

Response to breaches within minutes – OpenText is capable of responding to incidents within minutes, using its next generation V-SOC, its security appliance and its team equipped for broad data collection and ingestion of evidence from the endpoints, network and cloud. The team then employ advanced analytics, embedded machine learning, and custom workflows which quickly drive accurate root cause identification, remediation actions and security control improvement recommendations.

Detect threats across networks, endpoints and cloud – The methodology used enables a view across the organization, taking the investigative visibility of organizations' networks, endpoints and cloud presence. Using NextGen technologies including Ai and Machine Learning, the team offer near real-time threat detection which in turn, provides for timely remediation and thorough actionable recommendations.

Delivered leveraging OpenText solutions such as OpenText Forensic (EnCase), OpenText™ Threat Intelligence, Magellan, advanced analytics and machine learning combined with custom workflows and MITRE ATT&CK framework and overseen by Client Managers ensure organizations benefit from DFIR Services.

The Incident Response Retainer ensures quick responses to any incident and reduces time to remediate exponentially. The OpenText Cybersecurity Services team has the ability to react immediately, and come equipped with best in breed tools, know-how and extensive DFIR experience.

Not just incident response – a full DFIR service catalog OpenText provides onsite or remotely delivered services, leveraging its next generation V-SOC and forensic labs for faster breach response, cyber-attack analysis, proactive investigations, insider threats and more. The DFIR Services catalog includes:

- Incident Response Plan (IRP) development
- Runbooks
- Standard Operating Procedures (SOP) development
- Cyber simulation and tabletop exercises
- Next generation Security Information Event Management (SIEM) deployments
- Threat hunting
- Advanced digital forensics
- Insider threat investigations
- Reverse engineering and malware analysis
- Memory forensics
- Full Packet Capture (PCAP) and analysis
- Incident response
- Ransomware investigations
- Mobile forensics collection and analysis

Incident Response

For security breaches, cyber-attacks, insider threats or other investigations, OpenText delivers:

- Identification, triage, and validation of an incident
- Reporting on threats, impact details, and potential data exfiltration
- Hands on support for incident remediation and post incident activities
- Development of an increased skill level of the client team through collaborative investigations
- Feet on the ground’ incident response investigation and threat hunting
- Root cause analysis of the breach and incident response plan recommendations

Resources

Contact us ›

Incident Response Retainer

DFIR services are available across various programs and services agreements. Simple incident response retainers are also offered on pre-paid contracts at three competitive pricing levels1.

Level 1	Level 2	Level 3
40 Pre-paid hours USD 320/hr Hourly rate	**80** Pre-paid hours USD 310/hr Hourly rate	**150** Pre-paid hours USD 300/hr Hourly rate

Incident Response Retainer

With an Incident Response Retainer, organizations can meet their cyber security plan or insurance requirements within their budget while ensuring:

- Incident response hotline for incident response and escalation support
- Account Manager as DFIR Champion
- Response times
  - 8-hours - initial response and scoping
  - 24-hours - remote investigative support
  - 48-hours - on-site investigative support[2]
- **Not only incident response!** Conversion of banked hours for use against any Security Services in the Security Services catalog, including:
  - Security health check
  - Risk assessments
  - Threat hunting
  - Penetration testing
  - Cloud forensics
  - Managed Security Service Program (MSSP)
  - Tabletop exercises
  - Incident response playbook creation

For more information, please contact us at securityservices@opentext.com

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

1 Pricing on October 15th, 2020. For current hourly rate, please contact securityservices@opentext.com as pricing may change without notice.

2 Available throughout North America and Europe. Please confirm with your Account Manager availability in other regions.