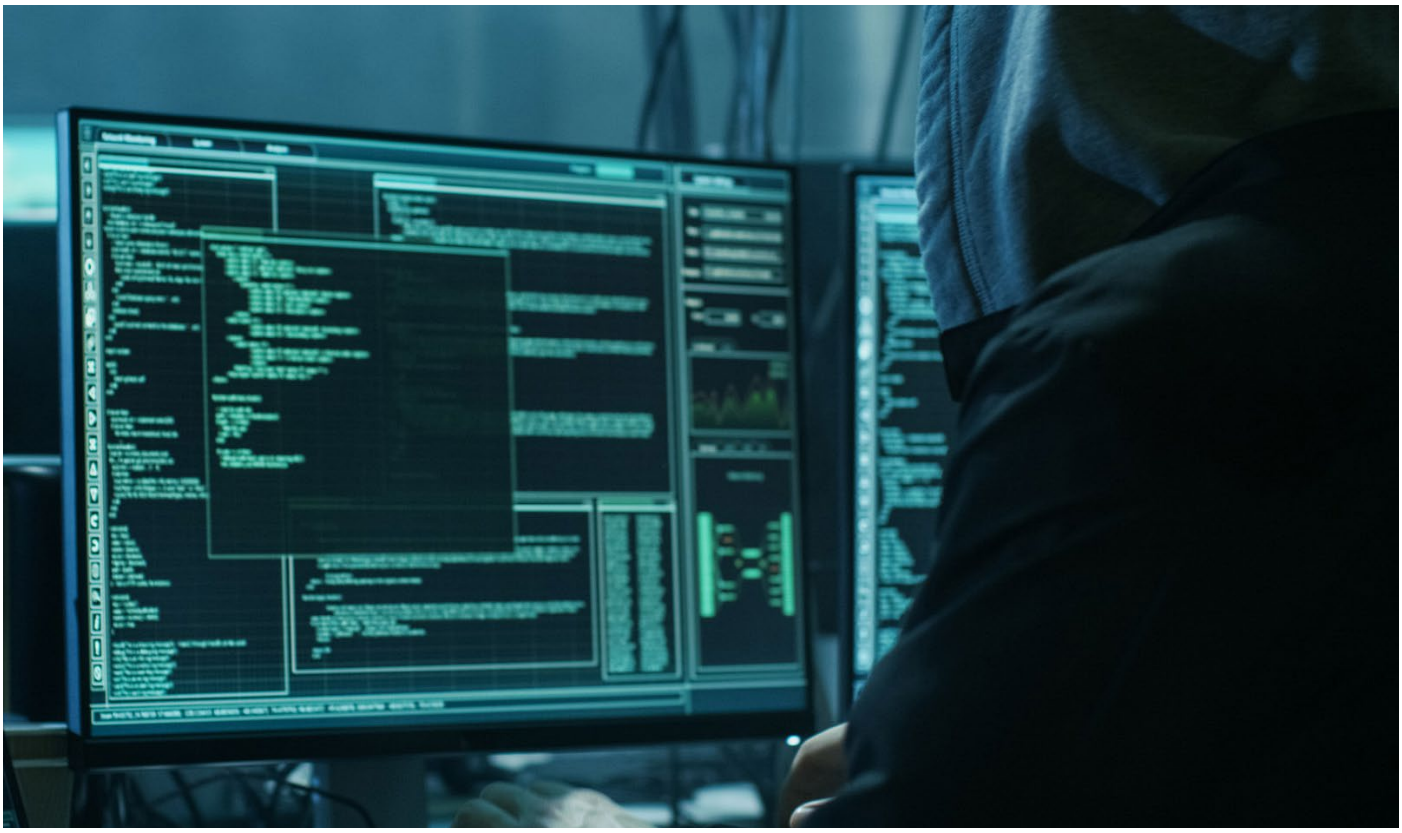
opentext™

SERVICE OVERVIEW

Digital Forensics & Incident Response (DFIR)

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



Benefits

- Rapid response to incidents
- Root cause analysis and defensible evidence management
- Enhanced security posture
- More than just an IR partner

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. Today, organizations of all sizes 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 27 years, the OpenText Cybersecurity Services team are professional investigators using the OpenText Digital Investigations and Forensics Portfolio and best-in-breed technologies. OpenText DFIR services combined with an Incident Response Retainer is a proactive approach to cybersecurity and helps organizations minimize the impact of an incident.

Rapid response to breaches

OpenText can respond to incidents within minutes, from its next-generation SOC, leveraging its investigation and forensic tools, and drawing from its expert team equipped for broad data collection and investigation of evidence from the endpoints, network and cloud. The team then employs advanced analytics and custom workflows, which quickly drive accurate root cause identification, remediation actions and security control improvement recommendations.

How do we deliver DFIR Services?

Our team leverages the OpenText end-to-end technology stack, including OpenText™ Endpoint Investigator, OpenText™ Information Assurance, OpenText™ Forensic Equipment, and OpenText™ Threat Intelligence. Over the last few decades, we also developed custom workflows and usage of the MITRE ATT&CK® framework to quickly identify the scope of the entire incident. Our DFIR services provide rapid response, in-depth root cause analysis, and a rapid return to an operational steady state, as well as an improved security posture.

Not just incident response—a full IR and post-IR service catalog

OpenText provides on-site or remotely delivered services, leveraging its next-generation and forensic labs for faster breach response, cyberattack analysis, proactive investigations, insider threats and more.

Incident Response specialties:

- Advanced digital forensics
- Insider threat investigation
- Threat hunting
- Reverse engineering and malware analysis
- Memory forensics
- Full Packet Capture (PCAP) and analysis
- Ransomware investigations
- Mobile forensics collection and analysis

Post Incident Response:

- Standard Operating Procedures (SOP) development
- Incident Response Plan (IRP) development
- Cyber simulation and tabletop exercises
- Runbooks against identity threat

Resources

Cybersecurity Catalog >

NextGen Cybersecurity Services >

Targeted DFIR evidence collections >

Incident Response scope

Overseen by our Service Program Manager, your DFIR Champion at OpenText, we cover all your needs during the IR lifecycle for any security breaches, cyberattacks, 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
- Lessons learned and continuous process improvement report

Incident Response Retainer

OpenText can deliver DFIR services across various programs and service agreements. Simple incident response retainers are also offered on pre-paid contracts at competitive pricing levels.

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

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

- Incident response hotline for incident response and escalation support
- Service Program Manager as DFIR Champion
- Response times*
    - 3 hours – Initial response with validation and scoping
    - 24 hours – Start of remote investigation support
    - 48 hours – On-site investigative support

Not only for incident response! Conversion of banked hours can be used against any Cybersecurity Services in our catalog, including:

- Security Health Check
- Risk Assessments
- Threat Hunting
- Security Testing/Penetration Testing
- Managed Security Services
- Tabletop Exercises
- Incident Response Playbook Creation

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

* Certain conditions apply. Talk to your OpenText Account Executive for all the details.