Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Digital Forensics and Incident Response (DFIR) Services, Q4, 2023

Market Insights, Competitive Evaluation, and Vendor Rankings

December, 2023

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of global Digital Forensics and Incident Response Services solution market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading Digital Forensics and Incident Response Services vendors in the form of SPARK Matrix™. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities, competitive differentiation, and market positions.

Market Dynamics and Overview

Quadrant Knowledge Solutions defines Digital Forensics and Incident Response (DFIR) services as a "set of cybersecurity services that are aimed at identifying, mitigating, and investigating cybersecurity incidents. It is a cybersecurity approach that merges two key disciplines, digital forensics involves investigating cyber threats to collect digital evidence for legal action against cybercriminals. On the other hand, incident response focuses on detecting and mitigating ongoing cyberattacks. These services involve proactive measures such as threat detection, containment, and recovery in the face of a security breach, as well as reactive digital forensics investigations that include evidence collection, analysis, and reporting".

In the ever-evolving landscape of cybersecurity threats, as organizations face a growing array of sophisticated cyber threats, the ability to swiftly detect, contain, and respond to incidents has become more important. The DFIR strategies are indispensable in minimizing the impact of security breaches, preserving the integrity of digital systems, and mitigating risks associated with data compromise. Now, while DFIR strategies can also be developed and implemented in-house, it presents the critical challenge of false positives and time to stay updated on the latest threats. Outsourcing these tasks helps organizations avoid these challenges. In addition, the proactive nature of DFIR services helps them recover from incidents and enables them to implement strategies for continuous improvement and build a strong cybersecurity posture.

The integration of newer technologies is playing a pivotal role in improving DFIR services. Machine learning and artificial intelligence have transformed threat detection by enabling more efficient analysis of large datasets and automating certain aspects of the incident response process. These technologies enhance the speed and accuracy of identifying anomalous activities, allowing for a more proactive and adaptive approach to cybersecurity. Additionally, advancements in cloud technologies have expanded the scope of DFIR services to address incidents occurring in virtual and cloud environments. Cloud-based forensic tools and techniques have become essential in investigating and responding to incidents involving data stored in distributed and dynamic environments.

DFIR services find diverse applications across industries. In the financial sector, DFIR is crucial for safeguarding against cyber threats targeting sensitive financial data and transactions. In healthcare, they ensure the security and privacy of

medical records. Moreover, critical infrastructure sectors, including energy, transportation, and telecommunications, rely on DFIR capabilities to protect essential services from cyber threats that could have far-reaching consequences. DFIR services help safeguard digital assets and ensure the resilience of organizational infrastructures.

The following are the key capabilities of a Digital Forensics and Incident Response (DFIR) Services solution:

- **Forensic Data Collection / Digital Evidence collection –** A DFIR service provides experts who play a crucial role in systematically collecting and preserving digital evidence. This process includes data extraction from various sources, such as servers, endpoints, network logs, and other relevant repositories. The meticulous preservation of this evidence is essential to ensure its adequacy in legal proceedings. DFIR specialists employ comprehensive techniques to gather, examine, and analyze data that is stored on-premises as well as in the cloud. This process involves scrutinizing information from networks, applications, data stores, and endpoints.

- **Threat Intelligence Integration-** DFIR services use threat intelligence feeds to understand cyber incidents better. The feeds include information about known attackers, how they operate, and signs of compromise. This knowledge allows DFIR teams to react to cyber threats faster and more effectively. Keeping up with evolving threats helps in dealing with ongoing incidents and making defenses stronger against future attacks. Using threat intelligence makes responses more focused and efficient, hence making the overall cybersecurity of an organization better.

- **Malware Analysis –** A DFIR service provides Malware Analysis capability. This analysis includes breaking down malicious software to grasp how it works, where it comes from, and what harm it can cause. This understanding is crucial for creating detection signatures and enhancing overall security measures. Dissection of malware allows analysts to gain insights into its behavior and structure, which aid in the development of effective countermeasures to identify and mitigate potential threats. This proactive approach is important for cybersecurity defenses and staying ahead of evolving malware threats.

- **Forensic Analysis-** The Forensic analysis capability enables analysis of collected evidence to assess the full scope of the incident, pinpoint the root cause, and comprehend the tactics, techniques, and procedures (TTPs) employed by attackers. This detailed examination is essential for formulating a response strategy that is both effective and targeted. An in-depth analysis of the incident enables analysts to understand how it occurred and develop proactive measures to prevent similar events in the future. This comprehensive approach is instrumental in crafting a robust response and mitigation plan, enhancing overall cybersecurity resilience.

- **Post-Incident Reporting and Continuous Improvement –** Once the incident is resolved, DFIR services provide detailed post-incident reports. These reports include findings from the investigation, lessons learned, and recommendations for improving security posture to prevent similar incidents in the future. DFIR services contribute to a cycle of continuous improvement by analyzing incidents and refining incident response plans and procedures based on lessons learned. This iterative process is crucial for staying ahead of evolving cyber threats.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Digital Forensics and Incident Response (DFIR) services vendors by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall DFIR services market. This study includes an analysis of the key Digital Forensics and Incident Response Services vendors, including Ankura consulting, Aon, AT&T, Atos, Blackberry, Booz Allen Hamilton, Check Point, Crowdstrike, CyberCX, Cybereason, Cyderes, eSentire, Google Cloud (Mandiant), Group-IB, Guidepoint, IBM, Kaspersky, Kroll, Kudelski, Mnemonic, NCC Group, Optiv Security, Orange Cyberdefense, Rapid7, SecureWorks, SecurityHQ, SecurityScorecard, Trustwave, Sygnia, TrustedSec, Unit42 by Palo Alto Networks, and Verizon.

Blackberry, Booz Allen Hamilton, Crowdstrike, Cybereason, eSentire, Group-IB, Kaspersky, Kroll, Optiv Security, Orange Cyberdefense, SecureWorks, and Unit42 by Palo Alto are the top performers and leaders in the global Digital Forensics and Incident Response services market and have been positioned as the top technology and service leaders in the 2023 SPARK Matrix™ analysis of the Digital Forensics and Incident Response services market. These companies provide sophisticated and comprehensive technology and service platforms to identify, manage, and respond to cybersecurity incidents, as well as detect, analyze, and mitigate security breaches and incidents in a timely and effective manner.

BlackBerry's Digital Forensics and Incident Response (DFIR) service is equipped with a team of experienced DFIR professionals who help organizations rapidly contain and remediate breaches, minimize business disruptions, and ensure compliance with regulatory requirements. The services cover a spectrum of functions, including digital forensics, incident response, threat hunting, and malware analysis. The team utilizes advanced tools and methodologies for investigating and mitigating security incidents. The focus is on proactive threat detection and efficient incident resolution. Through these services, BlackBerry aims to assist organizations in enhancing their cybersecurity defenses and managing the evolving cyber risks.

Booz Allen Hamilton provides integrated Digital Forensics and Incident Response (DFIR) services as a part of its consulting offerings. These services entail organized investigation, examination, and containment of cybersecurity incidents. The

company also maintains a specialized incident response team that tackles intricate and substantial breaches. Booz Allen's DFIR portfolio encompasses incident response, digital forensics, threat intelligence, and cybersecurity preparedness.

CrowdStrike offers Digital Forensics and Incident response through its Falcon Forensics platform and Incident Response services. CrowdStrike's Digital Forensics and Incident Response (DFIR) services are designed to cater to organizations of all sizes, offering an extensive suite of capabilities for the investigation and mitigation of cyberattacks. These services seamlessly integrate with CrowdStrike's Falcon platform to provide a unified solution. The DFIR services empower organizations to effectively respond to cybersecurity incidents. CrowdStrike's Falcon platform, in conjunction with DFIR services, ensures comprehensive visibility into and control over endpoints, networks, and cloud workloads. This integrated approach strengthens an organization's overall cybersecurity posture.

Cybereason's DFIR is a cloud-based solution designed to streamline the investigation and response to cyberattacks for organizations, promoting a more rapid and effective approach. The system collects and analyzes diverse forensic data, encompassing full disk images, memory dumps, and network traffic capture. The solution leverages this information to identify malicious operations (MalOps) and pinpoint all systems and users affected by an attack. Cybereason's Incident Response services empower organizations to promptly detect and remediate threats. Users benefit from a dedicated team of Incident Responders who provide continuous support throughout the entire process, ensuring project continuity and reducing Mean Time to Remediation (MTTR).

eSentire's DFIR service utilizes advanced techniques and skilled professionals to conduct comprehensive digital forensics investigations to identify the source, extent, and impact of security incidents. The company's incident response strategies are centered on containing breaches, eradicating threats, and implementing preventive measures to reduce the risk of future incidents. eSentire's DFIR services are designed to assist organizations in understanding and recovering from security breaches by employing a methodical and objective approach to handling cybersecurity incidents.

Group-IB specializes in Digital Forensics and Incident Response (DFIR) services. The company's DFIR services facilitate effective responses to security breaches, damage minimization, and incident prevention for organizations. Its capabilities encompass a range of services, such as malware analysis, reverse engineering, threat hunting, OSINT investigations, attack attribution, compromise assessment,

training and simulation, incident response readiness assessment, law enforcement support, post-incident support, and data collection and analysis. These DFIR services by Group-IB aim to provide a comprehensive solution for organizations facing cybersecurity challenges.

Kaspersky's Digital Forensics and Incident Response (DFIR) services offer a solution for organizations dealing with cybersecurity incidents. The company's professionals use advanced tools to conduct digital forensics investigations, aiming to identify the origin, scope, and impact of security events. The company's incident response strategies focus on containing breaches, eliminating threats, and implementing preventive measures. Kaspersky's DFIR services aim to assist organizations in understanding, managing, and recovering from security breaches with a systematic and objective approach to addressing cybersecurity challenges.

Kroll provides an extensive array of Digital Forensics and Incident Response (DFIR) services, encompassing incident response planning, digital evidence collection and analysis, incident containment and eradication, root cause analysis, remediation recommendations, and expert witness services. With both human expertise and technological capabilities, Kroll is equipped to swiftly identify potential threats, secure crucial data, and trace digital pathways.

Optiv Security provides Digital Forensics and Incident Response (DFIR) services that assist organizations in efficiently handling and reducing the impact of cybersecurity incidents. The company's services focus on examining security breaches, determining the scope of compromise, and swiftly implementing response measures to contain the incident. Optiv Security's DFIR offerings encompass an incident response retainer service, an incident management program, an incident response assessment, and a remediation service for vulnerability management programs.

Orange Cyberdefense's DFIR (Digital Forensics and Incident Response) services support organizations in investigating and recovering from cyber incidents. The company's DFIR team comprises experienced and certified professionals with a comprehensive understanding of cyber threats and incident response. The team leverages its expertise as well as its, the team has access to a global network of resources to address complex incidents effectively. Orange Cyberdefense'sDFIR services aim to assist organizations in navigating and mitigating the challenges associated with cyber incidents pragmatically.
SecureWorks offers DFIR capabilities through its Emergency Incident Response

service, a specialized offering designed to aid organizations during cybersecurity emergencies. The company's incident response team conducts comprehensive investigations to comprehend the nature and scope of the incident. The team closely works with the affected organization to mitigate risks and minimize potential damage. SecureWorks' Emergency Incident Response Service aims to enable organizations to navigate cybersecurity challenges efficiently and pragmatically.

Unit42 by Palo Alto Networks offers incident response services that constitute a comprehensive set of solutions aiding organizations of varied sizes in responding swiftly and effectively to cyberattacks. The company's team claims to comprise experts with extensive experience in investigating and responding to diverse cyberattacks, encompassing ransomware attacks, data breaches, and advanced persistent threats (APTs).

Aon, Atos, AT&T, Check Point, Google Cloud (Mandiant), IBM, Kudelski Security, NCC Group, Rapid7, and Verizon have been positioned among the primary strong contenders. These companies provide comprehensive technology capabilities and are gaining significant market traction in the global Digital Forensics and Incident Response services market. These companies are also mindful of the upcoming market trends and have outlined a comprehensive roadmap to tap into future growth opportunities. The other key vendors captured in the 2023 SPARK Matrix™ include Ankura Consulting, CyberCX, Cyderes, GuidePoint Security, Mnemonic, SecurityHQ, Security Scorecard, Sygnia, TrustedSec, and Trustwave.

All the vendors captured in the 2023 SPARK Matrix™ of the Digital Forensics and Incident Response services market are improving their capabilities for identifying, mitigating, and investigating cybersecurity incidents. Additionally, the vendors are focusing on increasing their customer base, geographical presence, and different industry verticals, as well as expanding use case support.

Key Competitive Factors and Technology Differentiators

Following are the key competitive factors and differentiators for the evaluation of Digital Forensics and Incident Response Services and vendors. While most of the Digital Forensics and Incident Response Services may provide all the core functionalities, the breadth and depth of functionalities may differ by different vendors' offerings. Some of the key differentiators include:

Cloud Forensics Expertise: Users should look for vendors offering expertise in cloud forensics. Owing to the increasing migration of organizations to the cloud, specialized vendors in cloud forensics are gaining a competitive edge. These vendors comprehend the distinctive challenges associated with investigating incidents in cloud environments and offer customized solutions for digital forensics and incident response in cloud-based systems. Their expertise lies in navigating the complexities of cloud infrastructure, ensuring effective collection and preservation of digital evidence, and addressing the specific nuances of cloud-based security incidents. As the demand for cloud services grows, these vendors play a crucial role in assisting organizations with forensic analysis and response strategies that are tailored to the dynamic nature of cloud computing.

Forensic Readiness Assessments: Users are suggested to look for vendors who are focusing on extending their services beyond incident response to provide forensic readiness assessments. These assessments play a proactive role in helping organizations prepare for potential incidents by ensuring that the essential tools, processes, and documentation are in place. The goal is to facilitate effective digital forensics when needed, enabling a swift and comprehensive response to security incidents. Forensic readiness assessments help organizations identify and address gaps in their capabilities to ensure that they are well-equipped to handle forensic investigations in a timely and efficient manner. This proactive approach enhances an organization's overall resilience to cyber threats by establishing a solid foundation for forensic activities, even before an incident occurs.

User Behavior Analytics (UBA): Users are suggested to look for vendors who are focusing on integrating User Behavior Analytics (UBA) into their services, utilizing machine learning and behavioral analysis to identify abnormal activities. This technology enhances the overall security posture by providing a dynamic and adaptive defense mechanism that goes beyond traditional rule-based systems, offering a better understanding of user activities and potential security threats.Automation and Orchestration: Users are suggested to look

for vendors prioritizing automation and orchestration capabilities to streamline incident response processes. This process involves automating repetitive tasks, orchestrating workflows, and facilitating quicker response times, all of which are paramount in the swiftly changing landscape of cyber threats. By leveraging automation, routine and time-consuming activities can be executed more efficiently, allowing cybersecurity teams to allocate their efforts toward more complex tasks. Orchestration ensures a coordinated and seamless workflow, enabling a more synchronized response to incidents. In the face of evolving cyber threats, the integration of automation and orchestration technologies becomes a strategic advantage, enhancing the agility and effectiveness of incident response efforts.

Cross-platform Compatibility: Users are suggested to look for vendors focusing on differentiating based on cross-platform compatibility. This compatibility ensures that their solutions work seamlessly across various operating systems and devices, encompassing not only traditional endpoints but also mobile devices, IoT devices, and other emerging technologies. The ability to adapt to a diverse technological landscape enhances the versatility of the solutions, allowing organizations to maintain comprehensive cybersecurity coverage across all facets of their infrastructure. In an era of diverse devices and evolving technologies, cross-platform compatibility becomes a strategic advantage, enabling organizations to address security concerns across a wide spectrum of computing environments.

Vendor's Expertise and Domain Knowledge: Organizations should evaluate vendors' expertise and domain knowledge in understanding their unique business problems, use cases, and industry-specific requirements. Organizations are advised to conduct a comprehensive evaluation of different Digital Forensics and Incident Response services vendors before making a purchasing decision. Users should employ a weighted analysis of the several factors important to their specific organization's use cases and industry-specific requirements.

Incident Simulation and Training: Users are suggested to look for vendors offering realistic incident simulation exercises and training programs. These initiatives enable organizations to assess and refine their incident response capabilities within a controlled environment, fostering continuous improvement and heightened readiness. By simulating real-world scenarios, teams can practice and enhance their response strategies, ensuring they are well-prepared for actual incidents. Incident simulation and training have become integral components of a comprehensive cybersecurity strategy, empowering organizations to stay ahead in the ever-changing landscape of digital security.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix™ provides a visual representation of market participants and strategic insights into how each supplier ranks as related to their competitors concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision-making, such as finding M&A prospects, partnerships, geographical expansions, and portfolio expansion.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix™.

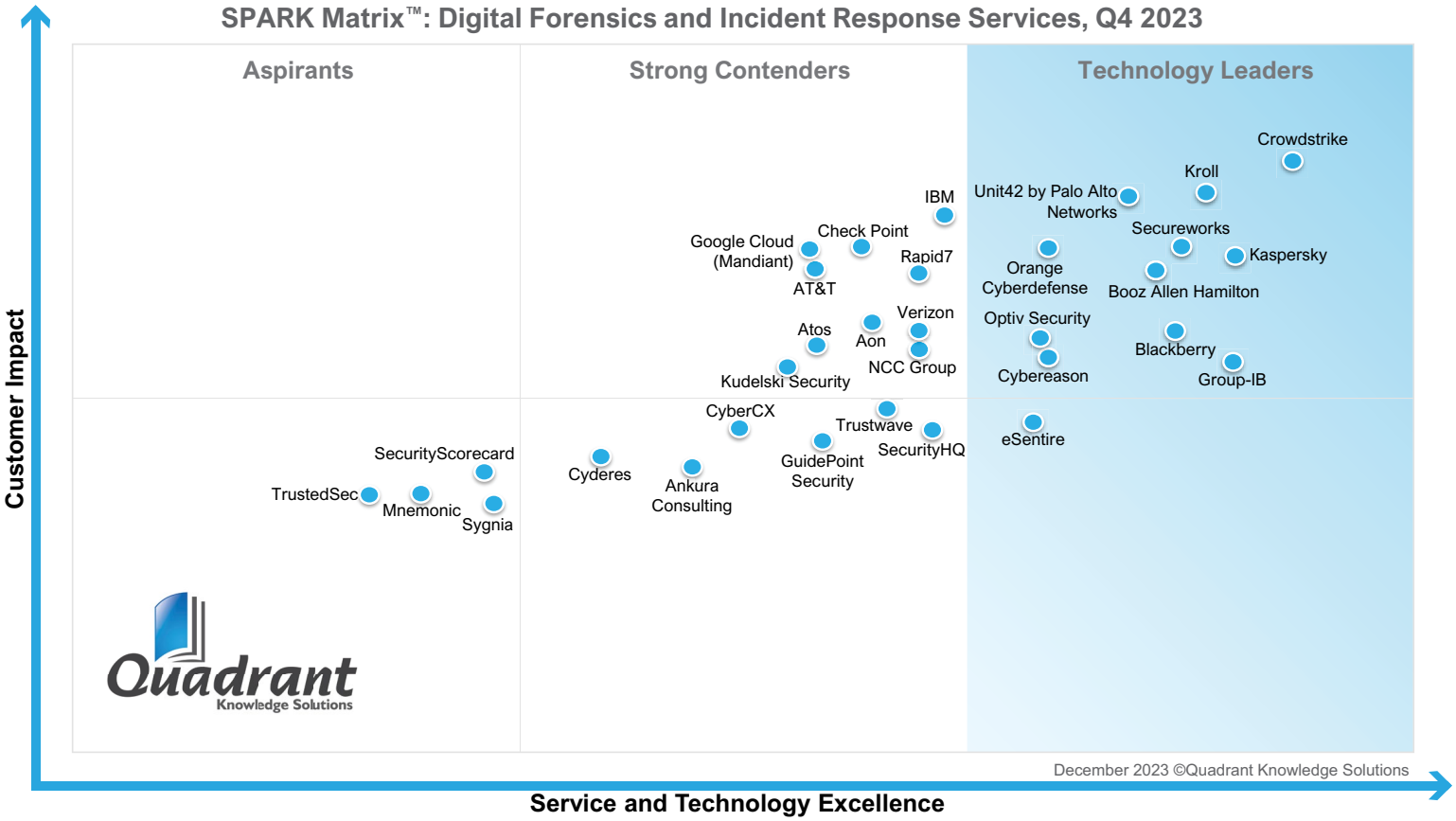
Service Excellence	Weightage
Sophistication of Service Capabilities	25%
Competitive Differentiation Strategy	25%
Industry Experience & Domain Knowledge	25%
Global Reach & Service Capabilities	15%
Vision & Roadmap	10%

Customer Impact	Weightage
Diversity of Client Base	25%
Market Presence	25%
Proven Record	25%
Customer Service Excellence	15%
Unique Value Proposition	10%

SPARK Matrix™: Digital Forensics and Incident Response (DFIR) Services

Strategic Performance Assessment and Ranking

Figure: 2023 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Digital Forensics and Incident Response (DFIR) Services



Vendor Profiles

Following are the profiles of the leading Digital Forensics and Incident Response (DFIR) service vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. The Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions regarding Digital Forensics and Incident Response Services and vendor selection based on research findings included in this research service.

Kaspersky

URL: https://www.kaspersky.co.in/

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Kaspersky also offers incident response services, which include Kaspersky Digital Forensics, Kaspersky Malware Analysis, and Kaspersky Incident Response.

Analyst Perspective

The following is the analysis of Kaspersky's capabilities in the Digital Forensics and Incident Response Services market:

- Kaspersky's Digital Forensics and Incident Response (DFIR) services are designed to help businesses respond to cybersecurity incidents efficiently. The company offers a team of experts and uses advanced tools and methods to identify, collect evidence, and analyze data related to security breaches. Kaspersky aims to assist organizations in understanding the nature and extent of the attacks they face.

- Kaspersky's Digital Forensics and Incident Response (DFIR) service offers capabilities that include digital forensics, which analyzes digital evidence related to cybercrime to provide a complete picture of an incident. Kaspersky also provides malware analysis that provides exhaustive information about the behavior and functionality of specific malware files. Kaspersky's DFIR service also includes incident response, which covers the entire incident investigation cycle to eliminate the threat.

- Along with the core capabilities, Kaspersky provides additional supporting services for their DFIR service. These services include a comprehensive portfolio of products and managed security services, allowing enterprises to actively detect and respond to cyber threats. The supporting products and services include threat intelligence, which provides technical, tactical, operational, and strategic intelligence, providing in-depth visibility into cyber

- threats targeting any organization. Kaspersky also provides an anti-targeted attack platform with endpoint detection and response that delivers all-in-one protection against complex and targeted attacks. Kaspersky also offers security assessment services, including penetration testing, red teaming, application and industry-specific security assessment. It also offers general and advanced training courses for employees, IT professionals, and security experts.

- Kaspersky provides expert guidance that includes Kaspersky Managed Detection and Response, Kaspersky Compromise Assessment, Kaspersky SOC Consulting, and Kaspersky Professional Services and Premium Support. The professional services and support cover the complete product cycle, from assessment through implementation to maintenance and optimization.

- Kaspersky differentiates its service offering from other vendors in the DFIR space by including intelligence sources that are not just limited to OSINT sources and include proprietary technologies gathering intelligence on threats that are currently active in real environments. Additionally, Kaspersky has a Global Emergency Response Team (GERT), which is a group of experts that has been investigating complex security incidents for organizations in every industry and region for more than ten years. GERT experts are certified in Incident Management, Digital Forensics, Malware Analysis, Network Security and Risk Assessment.

- From a geographical perspective, Kaspersky has a significant presence in the EMEA region, followed by META, APAC, and Latin America regions. Kaspersky's key industry verticals include the government and public sector, followed by BFSI, manufacturing, telecommunication, IT, transportation and media, healthcare, construction, education, and travel and hospitality industries. From a use case perspective, Kaspersky DFIR services support file encryption, suspicious system activity, data leaks, security tool alerts, money theft, and phishing.

Blackberry

URL: https://www.blackberry.com/us/en

Founded in 1984 and headquartered in Waterloo, Ontario, Blackberry is a provider of intelligent security software and services to enterprises and governments.

Blackberry provides cybersecurity services and offers consulting engagements that help clients secure their mission-critical operations and manage their endpoints, workspaces, and identities within a zero-touch, zero-trust architecture. Blackberry provides Digital Forensics and Incident Response services that include incident response/containment, incident response retainer, compromise assessment, forensic analysis, ransomware/ bitcoin negotiation, and business email compromise assessment.

Analyst Perspective

The following is the analysis of Blackberry's capabilities in the Digital Forensics and Incident Response Services market:

- BlackBerry Security Services include Incident Response (IR) and Forensics teams, which offer experienced support, artificial intelligence (AI) technology, and best practice methodologies to help organizations investigate, contain, and address security breaches. The IR and Forensics teams integrate AI into their tools and processes to rapidly generate preliminary results. This rapidness facilitates swift detection, forensic analysis, and containment of ransomware and advanced persistent threats, often initiated within hours of the initial data collection process.

- BlackBerry's incident response service includes investigative support and direction, malware analysis, forensics, log analysis, remediation planning and assistance, regular status reporting and project management-related activities, as well as reporting and/or presenting findings and recommendations. The service also consists of a compromise assessment service. This service has two phases: data collection and initial threat hunting, and targeted investigation. With compromise assessments, Blackberry also provides threat-hunting reports and attack surface reduction reports. BlackBerry's Incident Response (IR) teams swiftly generate preliminary results by utilizing artificial intelligence

in their tools and procedures. They can promptly initiate the detection and containment processes for ransomware and advanced persistent threats (APTs), often within hours.

- BlackBerry's digital Forensics service include Digital Forensics investigation that includes investigative scoping and project planning, forensic acquisition of electronic data, adhering to strict chain-of-custody procedures, analyzing acquired data, and reporting. BlackBerry Cybersecurity Services offers a comprehensive digital forensics service that includes a detailed investigation report. This report encompasses in-depth findings and recommendations essential for taking appropriate actions. It features an executive summary providing a concise overview of the findings, as well as a detailed technical section for a more comprehensive understanding. Furthermore, if applicable, the report includes specific recommendations tailored to the situation at hand.

- From a geographical presence perspective, BlackBerry has a strong presence in North America and Europe. From an industrial vertical perspective, BlackBerry's primary verticals include Government, financial services, professional services, utilities, manufacturing, healthcare, life sciences, education, transportation, and retail.

Booz Allen Hamilton

URL: https://www.boozallen.com/

Founded in 1914 and headquartered in McLean, VA, Booz Allen Hamilton is a global consulting firm offering a range of services, including strategy development, analytics, and technology solutions.

Booz Allen Hamilton's Digital Forensics and Incident Response (DFIR) services help organizations identify, contain, eradicate, and investigate actual or suspected cybersecurity intrusions.

Analyst Perspective

The following is the analysis of Booz Allen Hamilton's capabilities in the Digital Forensics and Incident Response Services market:

- Booz Allen Hamilton offers Digital Forensics and Incident Response (DFIR) services as part of its comprehensive consulting portfolio. These services involve systematic investigation, analysis, and mitigation of cybersecurity incidents. The firm has a dedicated incident response team that handles complex and significant breaches. Booz Allen's DFIR services include incident response, digital forensics, threat intelligence, and cybersecurity readiness.

- Booz Allen Hamilton's Digital Forensics and Incident Response (DFIR) team collaborates with a diverse range of organizations worldwide, offering extensive services tailored to identify, contain, eradicate, and investigate actual or suspected cybersecurity intrusions. The DFIR service offering by Booz Allen Hamilton utilizes a comprehensive set of capabilities that cover the entire incident response lifecycle. Their services include digital forensic investigations, cloud compromise investigations, ransomware recovery assistance, insider threat investigations, handling malware events, addressing network intrusions, mobile device forensics, compromise assessments, data mining, and manual review. Additionally, the DFIR team provides onsite and/or remote incident containment assistance, remediation and recovery assistance, emergency staff augmentation support, threat intelligence operations, pre-paid incident response retainer services, continuous cybersecurity testing,

and assessments, as well as tabletop exercises and wargaming activities. Booz Allen Hamilton's neutral and professional approach positions them as a trusted partner for organizations seeking expert assistance in the realm of cybersecurity.

- From a geographical presence perspective, Booz Allen has a significant presence in North America, followed by Europe, the Middle East and Africa, and Asia Pacific. From an industry vertical perspective, the company holds a strong presence in the aerospace and defense industry, followed by commercial, government, healthcare, financial services, energy, telecommunication, media and entertainment, technology, and education.

CrowdStrike

URL: https://www.crowdstrike.com/

Founded in 2011 and headquartered in Texas CrowdStrike is a global cloud-native cybersecurity provider that offers cloud-delivered protection for endpoints, cloud workloads, identities, and data. CrowdStrike offers Digital Forensics and Incident response through its Flacon Forensics platform and Incident Response services.

CrowdStrike's DFIR team is composed of experienced professionals with the experience of responding to a wide range of cyberattacks, including ransomware, data breaches, and targeted attacks. The team uses its expertise and the Falcon platform to quickly identify, contain, and eradicate threats.

Analyst Perspective

The following is the analysis of CrowdStrike's capabilities in the Digital Forensics and Incident Response Services market:

- CrowdStrike's Digital Forensics and Incident Response (DFIR) services offer a comprehensive suite of capabilities to help organizations of all sizes investigate and respond to cyberattacks. The service is combined with CrowdStrike's Falcon platform, which provides visibility into and control over endpoints, networks, and cloud workloads.

- CrowdStrike Falcon Forensics is an AI-powered platform that offers unified digital forensics. The platform supports CrowdStrike's incident response services by providing incident responders with the needed tools to investigate and respond to cyberattacks quickly and effectively. The Falcon Forensics platform provides automated data collection, enrichment, and correlation with intelligent data streams to streamline investigations. The platform also provides a wide-aperture collection system that facilitates incident response investigations by efficiently gathering diverse data types through a unified dissolvable collector. The platform also offers intuitive dashboards. In addition, Falcon Forensics is tightly integrated with the CrowdStrike Falcon platform. This integration allows incident responders to leverage the full power of the Falcon platform, including its threat intelligence and remediation capabilities.

- CrowdStrike provides Incident Response services through an Incident Response (IR) team. The team handles critical security incidents, resolving immediate issues and implementing a long-term solution. The team adopts an intelligence-led, collaborative strategy for investigations, integrating real-world incident response and remediation expertise with advanced technology on the cloud-based CrowdStrike Falcon® platform.

- Some of the capabilities offered by CrowdStrike's DFIR service include real-time incident response, which enables organizations to resume operations within days or weeks, minimizing the usual downtime that extends for months in traditional approaches. This approach accelerates the time to identify and resolve issues and reduces forensic costs. CrowdStrike also provides comprehensive investigation capabilities, as the DFIR team collects and analyzes evidence from across the organization's environment to determine the scope of the incident, identify the attackers, and understand their motivations. This information is used to develop a tailored remediation plan and to prevent future attacks.

- CrowdStrike differentiates its DFIR services from other vendors by offering a tailored approach for incident response. CrowdStrike collaborates with the organization's team to create a response and remediation strategy tailored to their operational requirements, existing investments, and resources. This approach ensures a comprehensive investigation and enables the development of a highly customized remediation plan. Additionally, CrowdStrike records the team's findings and strategic suggestions to improve the user's security posture. The recommendations are aligned with the organization's technological landscape, ensuring a balance between security objectives and business goals. CrowdStrike's services team provides a prioritized list of proposed modifications providing post-incident support.

- From a geographical presence perspective, CrowdStrike has a strong presence in North America, particularly the USA and Canada, followed by the UK, the Middle East, Turkey, Africa, Australia, and New Zealand. From an industry vertical perspective, the company has a presence across a wide variety of verticals, including healthcare, govt & public sectors, banking & financial services, retail & eCommerce, healthcare & life sciences, and energy & utilities. From a use case perspective, CrowdStrike supports incident response, threat hunting, security assessments, and incident preparedness.

Cybereason

URL: https://www.cybereason.com/

Founded in 2012 and headquartered in Boston, MA, Cybereason is a cybersecurity company that specializes in endpoint detection and response solutions. Cybereason assists organizations in proactively managing their cybersecurity posture and responding to cyber incidents promptly.

Cybereason Digital Forensic and Incident Response (DFIR) enhances the capabilities of the Cybereason Defense Platform by equipping defenders with essential tools for in-depth post-incident analysis, comprehensive remediation, and the eradication of embedded threats. Cybereason offers DFIR solutions as well as Incident Response professional services.

Analyst Perspective

The following is the analysis of Cybereason's capabilities in the Digital Forensics and Incident Response Services market:

- Cybereason DFIR is a cloud-based solution that helps organizations investigate and respond to cyberattacks more quickly and effectively. It does this by collecting and analyzing a wide variety of forensic data, including full disk images, memory dumps, and network traffic capture. The solution uses this data to identify malicious operations (MalOps) and to identify all of the systems and users impacted by an attack.

- Cybereason services offer Incident Response services that enable organizations to immediately identify and remediate threats. Cybereason offers users a dedicated team of Incident Responders that provide continuous support throughout the entire process to ensure project continuity and reduce Mean Time to Remediation (MTTR). Cybereason offers a team of expert threat hunters that is accessible round the clock, 365 days a year, ensuring that support is readily available when needed the most.

- Cybereason IR can be remotely deployed on all Microsoft-supported Windows platforms as well as most common Linux distributions. This wide compatibility

ensures that Cybereason's incident response capabilities can be effectively utilized across various operating systems, providing comprehensive coverage for organizations facing cybersecurity threats.

- Cybereason also provides post-incident reports with detailed insights and visibility into each MalOp (Malicious Operation), providing valuable information about vulnerabilities. These reports also include recommendations aimed at enhancing an organization's security posture.

- Cybereason Incident Response is differentiated from other Incident Response services by offering an AI-powered MalOp detection engine that can quickly identify malicious operations across all endpoints in the network. Additionally, Cybereason has a Forensics-as-a-code platform that organizations can use to automate many of the tasks involved in incident response, such as data collection and analysis.

- From a geographical presence perspective, Cybereason has a strong presence in North America, EMEA, and APAC. From an industrial vertical perspective, Cybereason's key verticals are financial services, healthcare, and advanced manufacturing.

eSentire

URL: https://www.esentire.com/

Founded in 2001 and headquartered in Waterloo, Canada, eSentire is a cybersecurity company that specializes in providing protection against digital threats for businesses. eSentire offers Digital Forensics and Incident Response (DFIR) services as part of its cybersecurity portfolio.

Analyst Perspective

The following is the analysis of eSentire's capabilities in the Digital Forensics and Incident Response Services market:

- eSentire's DFIR service leverages advanced techniques and skilled professionals to conduct thorough digital forensics investigations to identify the source, extent, and impact of security incidents. The company's incident response strategies focus on containing the breach, eradicating threats, and implementing preventive measures to minimize the risk of future incidents. eSentire's DFIR services aim to help organizations understand and recover from security breaches while ensuring a methodical and objective approach to handling cybersecurity incidents.

- eSenitre's DFIR service is supported by various capabilities that include the 4-Hour Remote Service Level Agreement (SLA) with a Retainer, which ensures prompt deployment of investigative tools and expert responders for businesses dealing with cybersecurity incidents. Additionally, eSentire provides critical visibility by deploying both commercially available and open-source tools, including eSentire's network, endpoint, and log technology, as necessary. This deployment aims to collect endpoint telemetry, full network packets, NetFlow, and log data from both on-premises and cloud environments. This multi-faceted approach enables a thorough examination of the situation from various vantage points, enhancing the depth and accuracy of the analysis process.

- The DFIR service also includes malware analysis, which involves the detection and analysis of malicious files and URLs, focusing on identifying suspicious activities. This in-depth analysis aims to provide a thorough examination of the

detected elements, enabling the generation of comprehensive and detailed reports. Along with malware analysis, digital forensic analysis is an important feature offered by eSentire. Through meticulous examination and analysis of digital evidence, this method aims to unravel the sequence of events leading to the incident, understand how it originated, identify the systems compromised during the breach, and discern the methods employed by the attacker to gain unauthorized access.

- eSentire also provides a robust reporting process that involves meticulously documenting the findings and impacts of the cyber investigation to capture a detailed chronicle of the steps taken. These reports provide comprehensive insights into the incident, outlining the specific findings of the investigation. eSentire also offers end-to-end incident management.

- eSentire also offers a Cybersecurity Investigation (CSI) team that provides access to a team of highly credentialed responders. Their collective expertise and backgrounds contribute to a deep and diverse skillset, ensuring that they are well-equipped to handle a wide range of cybersecurity incidents. The team also supports end-to-end incident management and covers the full incident response lifecycle.

- Regarding geographical presence, eSentire has a global presence in North America, particularly the United States, as well as the United Kingdom and the Asia Pacific region. eSentire serves a wide range of industries, including financial services, healthcare, manufacturing, retail, and government.

Group-IB

URL: https://www.group-ib.com/

Founded in 2003 and headquartered in Singapore, Group-IB is a provider of cybersecurity services and solutions that help users protect themselves against cyber threats and digital fraud. Group-IB specializes in Digital Forensics and Incident Response (DFIR) services that enable organizations to respond effectively to security breaches, minimize damage, and prevent future incidents.

Group-IB provides capabilities that include malware analysis and reverse engineering, threat hunting, OSINT investigations and attack attribution, compromise assessment, training and simulation, incident response readiness assessment, law enforcement support, post-incident support, and data collection and analysis as part of its DFIR services.

Analyst Perspective

The following is the analysis of Group-IB's capabilities in the Digital Forensics and Incident Response Services market:

- Group-IB's DFIR services assist the user organizations in effectively responding to cybersecurity incidents. Group-IB's DFIR services provide organizations with the necessary expertise to understand and address cyber threats, ensuring a methodical and comprehensive response to incidents. The Group-IB team uses a suite of tools and methodologies to detect, analyze, and address security breaches.

- Group-IB provides various capabilities with its DFIR services, including leveraging Open-Source Intelligence (OSINT), through which the team gathers, analyzes, and interpret data from publicly available sources to aid in investigations and attribute attack to their origin. This interpretation provides valuable context and helps in planning strategic responses. Group-IB also offers users the capability to conduct comprehensive compromise assessments to identify any indicators of compromise within the digital environment.

- Group-IB's data collection and analysis capability uses a range of forensic tools and methodologies to extract, preserve, and interpret data and ensure it

can be used for effective incident response, recovery, and legal proceedings. Additionally, Group-IB offers law enforcement support, which assists law enforcement agencies, INTERPOL, EUROPOL, and AFRIPOL, with technical expertise and knowledge in digital forensics and incident response. Group-IB provides support from a range of providing expert testimony to conducting advanced technical analyses to support cybercrime investigations.

- Group-IB's team of experienced reverse engineers provides detailed malware analysis, dissecting malicious code to understand its origin, functionalities, and potential impacts, that are factored into the company's incident response strategy. Group-IB's DFIR services also include threat-hunting capabilities, which involve hunting for potential threats within the digital environment using advanced tools, including the Group-IB MXDR platform and intelligence. This measure helps detect and mitigate cyber threats before they can escalate into severe incidents.

- Additionally, the Group-IB team provides robust training programs and simulation exercises to help organizations prepare for potential cyber threats. These trainings help the customers learn effective incident response strategies, improve their skills, and validate existing incident response plans. Another capability offered by Group-IB is incident response readiness, which analyzes procedures, tools, and teams to assess readiness, identify gaps, and recommend improvements to ensure they are prepared for an incident. The company also helps conduct a detailed post-mortem analysis, identify causes, and implement changes to prevent recurrence.

- Group-IB also offers a Unified Risk Platform that includes its own MXDR, Attack Surface Management, Threat Intelligence, Business Email Protection, Fraud Protection and Digital Risk Protection solutions. Group-IB also provides Human-oriented security services based on knowledge-sharing and GROUP-IB DNA sharing with end clients.

- Group-IB has a significant presence in the EMEA market, followed by North America and the Asia Pacific region. It also holds a strong position in the BFSI, telecommunication, and government and public sector industries, followed by e-commerce, healthcare, manufacturing, retail, transportation and media, food and beverages, entertainment, and gaming industries. Some of the key use cases of Group-IB include ransomware incident response, multi-APT intrusion incident response, and continuous data leak investigation.

- Group-IB's future roadmap focuses on streamlining its range of products and services by integrating them into a single interface on a unified platform, not only to simplify the user experience but also to enhance collaboration and coordination across different service areas. The company also aims to incorporate adjacent competencies such as red teaming, consulting, and training into its service offerings to provide a more comprehensive and proactive approach to cybersecurity.

Kroll

URL: https://www.kroll.com/en

Founded in 1932 and headquartered in New York, NY, Kroll provides a wide range of risk and financial advisory services, including valuation, corporate finance and restructuring, investigations and disputes, cyber security, and business services. The company's DFIR services help organizations protect their digital assets, investigate security incidents, and respond to cyberattacks.

Kroll has a team of experienced DFIR professionals with a deep understanding of the latest cyber threats and the latest digital forensics tools and techniques. The team also helps organizations develop and implement customized DFIR solutions that meet the specific needs of each organization.

Analyst Perspective

The following is the analysis of Kroll's capabilities in the Digital Forensics and Incident Response Services market:

- Kroll offers a wide range of DFIR services, including incident response planning and preparation, digital evidence collection and analysis, incident containment and eradication, root cause analysis and remediation recommendations, and expert witness services. Kroll possesses the necessary human and technological capabilities to promptly identify potential threats, safeguard important data, and follow digital trails.

- Kroll provides 24x7 incident response that is supported by its global network of cybersecurity and digital forensic experts who can quickly deploy remote solutions or assemble an onsite team. This ability aids organizations in containing incidents and deciding on appropriate follow-up actions.

- Kroll offers various capabilities that support their Digital Forensics and Incident Response services. These capabilities include threat detection, which uses a team of cybersecurity consultants and forensic analysts specializing in conducting live system memory analysis and forensic examinations of developing malware threats. This expertise supports clients in enhancing their response strategies against cybersecurity challenges. Kroll also uses advanced forensic software and procedures to gather and safeguard data

from all parts of a client's system, including servers, laptops, and mobile devices. The company ensures meticulous evidence handling by utilizing data recovery tools and forensic methodologies that are backed by case law.

- Kroll also provides Payment Card Industry (PCI) forensic investigators, who utilize advanced tools and techniques to ascertain potential compromises in cardholder data and investigate the methods behind such compromises. Additionally, Kroll's Cyber Risk team has a track record of conducting investigations mandated by the PCI Security Council, demonstrating their expertise in the field. Additionally, for incident recovery and remediation, Kroll offers related services, including device and server reimaging, directory rebuilding, network hardening and segmentation, hardware upgrades, and patch management.

- Kroll differentiates its service from other vendors by providing threat simulations. Kroll has established a structured seven-step process for guiding tabletop exercises (TTX) tailored to organizations of varying sizes, industries, and complexities. Engaging in a Kroll TTX enables an organization's response team to clearly outline and practice their roles. This preparation equips them to respond more confidently and effectively in the event of an incident. Along with this, Kroll supports AI-fueled threat intelligence analysis via CyberDetectER Dark Web.

- Kroll has a significant geographical presence in the US Europe, the Middle East and Africa, and the Asia-Pacific region. Kroll offers its services to a wide range of industries, including financial services, healthcare, technology, energy, manufacturing, retail, consumer goods, media and entertainment, and government sectors. From a use case perspective, Kroll's DFIR service supports protecting intellectual property, preparing for and responding to regulatory investigations, investigating fraud and misconduct, and conducting due diligence.

Optiv Security

URL: https://www.optiv.com/

Founded in 2015 and headquartered in Denver, CO Optiv Security is a cybersecurity solutions provider offering a range of services, including cybersecurity consulting, threat intelligence, incident response, identity and access management, and managed security services.

Optiv Security offers Digital Forensics and Incident Response (DFIR) services that are designed to help organizations effectively manage and mitigate cybersecurity incidents. The services focus on investigating security breaches, identifying the extent of the compromise, and implementing rapid response measures to contain the incident. Optiv Security's DFIR service includes an incident response retainer service, an incident management program, an incident response assessment, and a vulnerability management program remediation service.

Analyst Perspective

The following is the analysis of Optive Security's capabilities in the Digital Forensics and Incident Response Services market:

- Optiv Security's DFIR service involves a systematic analysis of digital evidence, including logs, network traffic, and system artifacts, to uncover the root causes of incidents. The company has a team of professionals who follow industry-standard methodologies to conduct thorough investigations, enabling clients to make informed decisions regarding incident containment and remediation. Additionally, Optiv Security takes a proactive approach to cybersecurity challenges by providing guidance on improving security postures to prevent future incidents.

- Optiv Security's DFIR service is supported by various capabilities, including a formal incident response program. Optiv Security assesses the organization's existing controls, procedures, tools, and technology within the context of the current threat landscape. Subsequently, they develop or update playbooks, processes, escalation plans, and other necessary elements. The service is continuously improved based on lessons learned from resolved incidents.

The resulting program covers crucial incident response steps, including identification, protection, detection, response, and recovery integrated to mitigate cyber risk effectively.

- Optiv Security also offers incident management assessments. These assessments take into consideration the prevailing threat landscape, aiming to minimize enterprise risk by evaluating the client's incident response capabilities. Their incident management framework incorporates various security controls, all derived from widely accepted industry standards such as NIST SP 800-61. The incident assessment is a part of Optiv's incident management program. The program is a systematic approach that enhances consistency, reduces uncertainty, and improves the ability to identify, compensate for, and remediate incidents by providing clear priorities and procedures.

- Optiv Security has a significant presence in North America, followed by Europe, Asia Pacific, the Middle East and Africa, and South America. The company has a presence in various industries, including financial services, healthcare, energy, technology, retail, manufacturing, government, and education.

Orange Cyberdefense

URL: https://www.orangecyberdefense.com/

Founded in 1988 and headquartered in Nanterre, Paris, Orange Cyberdefense is a cybersecurity service provider that offers a range of services, including managed security services, consulting services, and security solutions and services, that are designed to protect businesses and organizations from cyber threats.

Orange Cyberdefense offers DFIR services through its computer security incident response team (CSIRT), which handles security incidents from detection to closure and recovery.

Analyst Perspective

The following is the analysis of Orange Cyberdefense's capabilities in the Digital Forensics and Incident Response Services market:

- Orange Cyberdefense offers DFIR (Digital Forensics and Incident Response) Services that help organizations investigate and recover from cyber incidents quickly and effectively. Orange Cyberdefense's DFIR team, as per the company, is composed of experienced and certified professionals with a deep understanding of cyber threats and incident response. The team has access to a global network of resources that can be brought to bear on even the most complex incidents.

- Orange Cyberdefense's DFIR services support a wide range of capabilities, including Intelligence-led incidents that gather Indicators of Compromise (IOCs) from the Orange Cyberdefense Threat Intelligence backbone. Their CSIRT is connected with other CERT components, including the Cybercrime Monitoring team responsible for monitoring the open, deep, and Dark web, as well as their network of Security Operations Centers (SOCs) and Cyber Security Operations Centers (CyberSOCs). The intelligence operations within the CSIRT leverage the available cyber threat intelligence, enabling them to offer informed guidance on preparing for future incidents and providing specific context during an ongoing incident.

- Orange Cyberdefense DFIR services help organizations detect and respond to cyber incidents quickly and effectively. The team uses a variety of tools and techniques to identify suspicious activity, including endpoint detection and response (EDR), intrusion detection systems (IDS), and security information and event management (SIEM) systems. Once an incident is detected, the team will work to contain it, eradicate the threat, and help the organization recover from it.

- Additionally, Orange Cyberdefense DFIR service provides security consulting, which enables organizations to assess their security posture, identify and mitigate risks, and develop and implement security strategies. The team, as per the company, has a deep understanding of cybersecurity best practices and can help organizations improve their security posture. Also, the DFIR service provides complete incident reports, fast isolation, and 24x7 availability.

- From a geographical presence perspective, Orange Cyberdefense has a significant presence in Europe, followed by the US, Africa, the Middle East, and Asia-Pacific. From an industry vertical perspective, the company's primary verticals are manufacturing, energy, utilities, transportation, Oil and gas, chemicals, pharmaceuticals, and food and beverages.

Secureworks

URL: https://www.secureworks.com/

Founded in 1999 and headquartered in Atlanta, GA, Secureworks provides a wide range of security solutions and services that help organizations protect their networks, data, and applications from cyberattacks.

Secureworks offers DFIR services through the Secureworks Emergency Incident Response and Incident Management retainer services

Analyst Perspective

The following is the analysis of Secureworks's capabilities in the Digital Forensics and Incident Response Services market:

- Secureworks provides DFIR capabilities through its Emergency Incident Response service. Secureworks Emergency Incident Response Service is a specialized offering tailored to assist organizations during cybersecurity emergencies. The incident response team conducts thorough investigations to understand the nature and extent of the incident. The team focuses on collaboration, working closely with the affected organization to mitigate risks and minimize potential damage. Secureworks Emergency Incident Response Service enables organizations to navigate cybersecurity challenges efficiently.

- Secureworks provides incident response capabilities for rapid investigation, analysis, and remediation of cyberattacks. These capabilities include incident command that involves Incident response professionals offering expert guidance to maintain a business-oriented approach and minimize risks during the response process, encompassing investigation and remediation efforts.

- SecureWorks also provides remediation guidance capability through its Emergency Incident Response service. The capability involves Experienced incident response specialists, who provide guidance and assistance in the remediation process, swiftly restoring the user's business operations and enhancing their security measures to prevent future attacks. Additionally, Secureworks also utilizes malware analysis, reverse engineering, digital

forensics, active directory proficiency, adversarial testing skills, as well as deep web and dark web surveillance.

- Secureworks differentiates its incident response service from other vendors by utilizing Secureworks Taegis™ XDR. The Taegis security analytics accelerates the investigation process and enhances the speed of response and recovery efforts. Secureworks also leverages its Incident Response (IR) experts, the Cyber Threat Unit (CTU), and adversarial security testers to offer valuable insights into threat actors, providing enhanced context to bolster response, remediation, and recovery efforts.

- From a geographical perspective, Secureworks has a strong presence in the USA, followed by Europe and Australia. From the industry vertical perspective, primary verticals for Secureworks include healthcare, banking and financial services, manufacturing, and retail. From a use case perspective, Secureworks Incident Response supports mitigation of ransomware and cyber extortion, business email compromise, insider threats, and advanced persistent threats.

Unit42 by Palo Alto Networks

URL: https://unit42.paloaltonetworks.com/

Founded in 2005 and headquartered in Santa Clara, CA, Unit 42 is a division of cybersecurity giant Palo Alto Networks that provides threat intelligence, incident response services, and cyber risk management. Unit42's incident response team helps organizations respond to cyberattacks quickly and effectively. Unit42 experts helps users contain attacks, investigate causes, and recover from the damage.

Analyst Perspective

The following is the analysis of Unit42's capabilities in the Digital Forensics and Incident Response Services market:

- Unit 42 incident response services are a comprehensive set of services that help organizations of all sizes to respond to cyberattacks quickly and effectively. Unit 42 states it possesses a team of experts with extensive experience investigating and responding to cyberattacks of all types, including ransomware attacks, data breaches, and advanced persistent threats (APTs).

- Unit42 has a wide range of supporting service capabilities for their DFIR services. For Digital Forensics, some of the capabilities include digital investigation, where the process involves gathering, examining, retrieving, and documenting information obtained from digital media using scientific techniques to ascertain the events that occurred on the media or how it was utilized. Unit 42's Digital Forensics service supports insider threat and departing employee investigation, which involves examining instances of trusted employees abusing their privileged access, including identifying the data they accessed or misused, as well as detecting any unauthorized actions taken by these insiders.

- Unit 42's Digital Forensics also includes litigation support, which examines digital evidence and discovery, providing expert opinions to the decision-maker, which may be presented in reports, declarations, depositions, or open court testimony. Additionally, it provides structured data investigation, which is Gathering and evaluating data from both SQL and NoSQL database systems, as well as external logs, for analysis and examination.

- Unit 42's incident response services offer capabilities that include ransomware investigation, which addresses and mitigates a ransomware attack by containing the threat, identifying the root cause, determining the window of compromise, analyzing attacker activity, and assessing the extent of sensitive information exposed. Along with this, Unit 42 provides cloud breach response, business email compromise, and web app compromise.

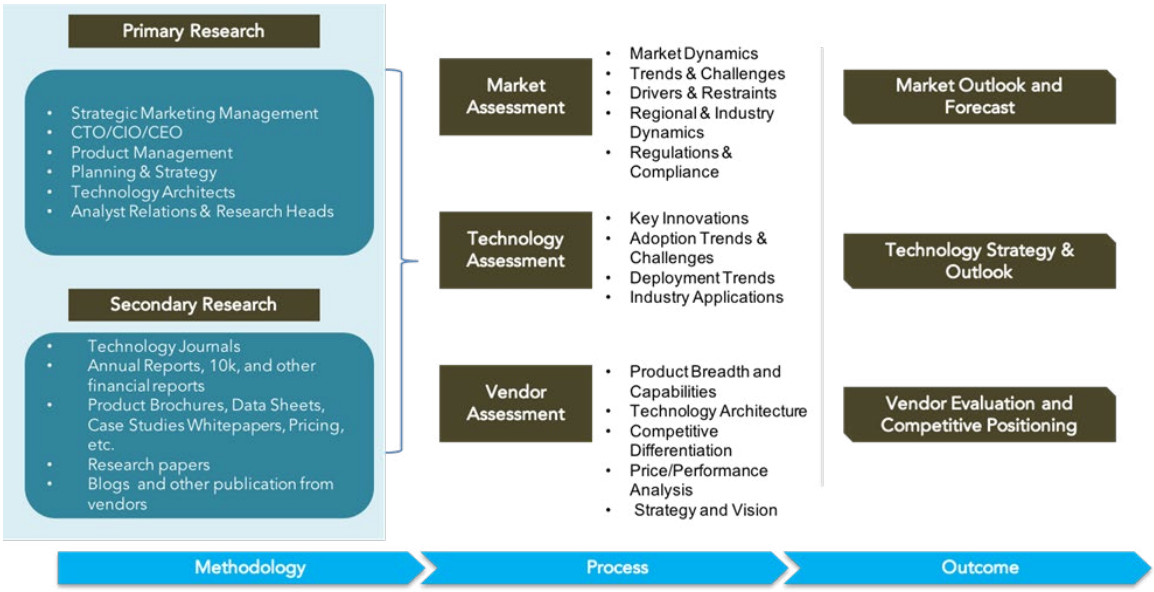
- Unit 42 also supports advanced persistent threat investigations that address a suspected Advanced Persistent Threat (APT) incident and help users recover from such threats. It achieves this by containing the threat, identifying the root cause, determining the window of compromise, analyzing attacker activity, and assessing the extent of sensitive information exposed. Unit42 incident response provides malware analysis, which examines malware samples through open-source intelligence, sandboxing, and reverse engineering techniques to understand their behavior and functionality. The service also offers a PCI/ Credit Card Breach Investigation that involves containing the threat, identifying the root cause, determining the window of compromise, analyzing attacker activity, and quantifying the credit card information exposed in accordance with PCI (Payment Card Industry) standards.

- Unit42 also provides other supporting services. These include MDR service, which assists in monitoring security events within your Cortex XDR environment. It operates by proactively detecting and responding to threats, aiming to minimize their impact swiftly and efficiently. Unit42 also provides a managed threat-hunting service that employs top-tier threat hunters in combination with Cortex XDR technology, which operates across endpoint, network, and cloud data sources. This integrated approach helps uncover attackers and enhance overall security measures.

- From a geographical presence perspective, Unit42 has a significant presence in the North America region, followed by Europe, Asia Pacific, Middle East and Africa, and Latin America. From an industry vertical perspective, Unit42 has a strong industrial presence in financial services, healthcare, government, retail, manufacturing, technology, education, energy and utilities, telecommunication, transportation, and media and entertainment industries. From a use case perspective, Unit42 supports a broad range of use cases, including intellectual property theft, supply chain attacks, nation-state attacks, advanced persistent threats, cyber espionage, security assessments, threat hunting, and cyber-insurance.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

SPARK Matrix: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.

Client Support

For information on hard-copy or electronic reprints, please contact Client Support at

ajinkya@quadrant-solutions.com | www.quadrant-solutions.com