BlackBerry
Intelligent Security. Everywhere.

Data Sheet

Incident Response and Forensics

Expert Support for Investigating, Containing, and Remediating Security Breaches

Threat actors are continually increasing the quantity and sophistication of their attacks with tactics, techniques, and procedures (TTPs) that are explicitly designed to evade detection. In this high-risk climate, prudent organizations prepare for the near-certainty of a breach with an incident response plan designed to minimize the resulting damage and reduce the potential liability. Outsourcing incident management can be a sensible and cost-effective approach for achieving both objectives.

BlackBerry® Security Services Incident Response (IR) and Forensics teams provide the expert support and direction organizations need to investigate, contain, and remediate security breaches and prevent them from recurring. There is no requirement to be an existing BlackBerry customer to receive this support. BlackBerry Security Services are available to every organization.

206 DAYS

To Identify a Data Breach

+

73 DAYS

To Contain It

In 2019, it took organizations an average of 206 days to identify a data breach and another 73 days to contain it, a nearly 5% increase over the year before.

Source: 2019 Cost of a Data Breach Report. IBM Security

Service Overview

By integrating artificial intelligence (AI) into their proprietary tools and processes, BlackBerry Security Services IR and Forensics teams produce preliminary results quickly. Detection, forensic analysis, and containment of ransomware and advanced persistent threats can begin within hours of completing initial data collection.

BlackBerry Security Services teams utilize best practice IR and forensic investigation methodologies to trace kill chains, identify exploited vulnerabilities, assess impacts, and craft remediation plans. Areas of focus include:

Incident Response

- Investigative support and direction
- Malware, forensic, and log analysis
- Remediation planning and assistance
- Regular status reporting and project management-related activities
- Reporting and/or presenting findings and recommendations

Forensics Investigation

- Investigative scoping and project planning
- Forensic acquisition of electronic data
- Adhering to strict chain-of-custody procedures
- Analyzing acquired data
- Reporting and/or presenting findings and recommendations

Deliverables

At the conclusion of the BlackBerry Security Services IR engagement, clients receive a comprehensive report of findings that includes:

- A kill chain timeline tracing the attacker's actions on the network
- Names and details of identified threats
- The hosts and endpoints compromised during the incident
- The initial infection vector identified through root cause analysis
- A strategic remediation roadmap with priorities and assigned owners
- Detailed recommendations for increasing the client's overall cyber resilience

A breakout presentation can be scheduled for the client's leadership, management, and technical stakeholders to provide a forum for discussing the security issues raised during the engagement and promoting a more security-aware culture.

Expected Business Benefits

BlackBerry Security Services teams' multi-faceted approach to IR afford clients the following benefits:

- **Rapid Detection and Remediation:** By leveraging BlackBerry® AI technology and processes, BlackBerry Security Services IR teams produce preliminary findings quickly, often within hours of beginning their analysis.
- **Seamless Collaboration:** The scope and objectives for each BlackBerry Security Services IR engagement are detailed and documented in advance to enable seamless collaboration between the BlackBerry Security Services and client IR teams.
- **Low-Touch Data Collection:** Data collection methods are efficient, transparent, and leave minimal artifacts behind.

Skill-Building Opportunities for Internal Security Teams:

- The strategic malware, forensic, and log analysis reporting conducted by BlackBerry Security Services IR experts provides internal teams with invaluable opportunities for education and skill-building.

To Learn More

For more information about BlackBerry Security Services for Incident Response and Containment, please request a consultation or call **+1-888-808-3119** for immediate assistance.

About BlackBerry Security Services

BlackBerry Security Services consulting engagements enable clients to secure their mission-critical operations and manage their endpoints, workspaces, and identities within a Zero Touch, Zero Trust architecture. Our consultants provide the in-depth knowledge and investigative experience organizations need to minimize their cyber risk exposure and defeat persistent, well-funded attacks. Working together, we help clients address the full spectrum of cybersecurity challenges and construct a strong and effective security posture utilizing prevention-first methodologies. Please visit our consulting landing zone for the complete list of BlackBerry Security Services solutions.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

PS20-0408 | 200715