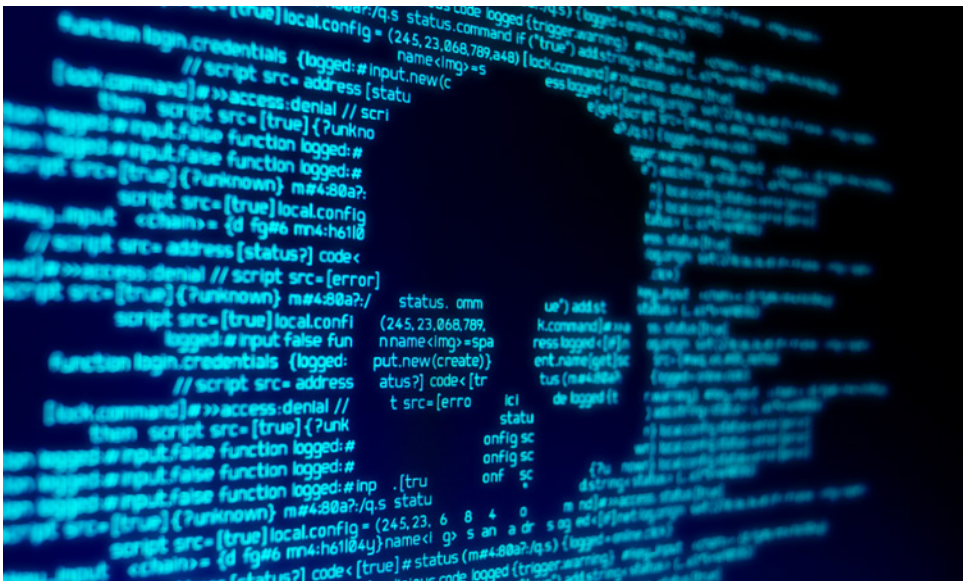
BlackBerry
Intelligent Security. Everywhere.

Data Sheet

Compromise Assessment

Identify and Assess Past Breaches To
Proactively Prevent Future Incidents



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 environment, how can an organization know with certainty whether its cyber defenses have already been compromised? If so, how quickly can the nature, extent, and impact of the breach be determined, and actions taken to terminate the attack and remediate the damage?

Many organizations today lack the necessary visibility, toolsets, resources, and experience needed to answer these questions with confidence. The trends are disquieting. 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.[1]

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*

1 2019 Cost of a Data Breach Report. IBM Security

A BlackBerry® Security Services Compromise Assessment (CA) can alleviate this uncertainty by providing clients with a comprehensive analysis of their cyber risk exposure. Enterprise-wide data is collected and analyzed for evidence of suspicious activity. Indicators of compromise (IOCs) are prioritized for in-depth investigation based on the risks they pose to the client's network environment and business operations. Key areas of focus include:

- Data exfiltration and sabotage
- Command and control activities
- User authentication abnormalities
- Malware persistence mechanisms
- Vulnerable network host and application configurations

If evidence of a past breach is discovered, BlackBerry Security Services CA experts can determine when, where, and how it occurred, and provide tactical recommendations for preventing a recurrence. If a breach is currently in progress, the BlackBerry Security Services CA team can transition seamlessly into incident response (IR), tracing the kill chain, identifying TTPs, and assisting with remediation and cleanup.

By integrating artificial intelligence (AI) technology into their proprietary tools and processes, BlackBerry Security Services CA teams produce preliminary results quickly, often detecting commodity attacks and advanced persistent threats within hours of completing initial data collection. At the conclusion of the engagement, clients receive a report detailing the threat hunting findings, and recommendations for increasing their cyber resilience and reducing their attack surface. There is no requirement to be an existing BlackBerry customer to secure this support. BlackBerry Security Services are available to every organization.

Service Overview

BlackBerry Security Services CA consultants employ an AI-enriched best practices methodology for assessing environmental risks, identifying security incidents, and uncovering ongoing threat actor activity in a network environment. All BlackBerry Security Services CA engagements address the twin domains of threat hunting and attack surface reduction, and proceed from initial to targeted assessment phases.

Initial Assessment

In the initial assessment phase, the client is provided with a lightweight package of software and scripts for capturing the data the BlackBerry Security Services CA team will need to hunt for anomalous behaviors, IOCs, and other risks to the environment. This typically includes filesystem metadata from endpoints, log data from network devices, event and alert data from ancillary security systems, and more. Next, the BlackBerry Security Services CA team utilizes proprietary cloud-based tools and methodologies to normalize, contextualize, enrich, and format the data. The resulting forensic artifacts are processed with a proprietary analytics engine and are reviewed to identify hosts of interest and activities that require further investigation.

Targeted Assessment

During the targeted assessment phase, standalone executables are deployed to the hosts of interest to gather more in-depth forensic data about the suspicious activity flagged during the initial assessment. If an active breach is detected, the BlackBerry Security Services CA team can immediately transition into incident response, utilizing best practice IR methodologies to trace the kill chain, document exploited vulnerabilities, assess impacts, and craft remediation plans.

Deliverables

At the conclusion of the engagement, the BlackBerry Security Services CA consulting team will submit a comprehensive report of its findings and recommendations:

- **Threat Hunting Findings:** If a past or current compromise has been detected, the report will detail its nature, extent, and impacts on the environment.
- **Attack Surface Reduction Findings:** Strategic and tactical recommendations for improvements to the enterprise's security posture will be detailed, along with a risk-prioritized assessment of attack surface reduction opportunities.

A breakout presentation can be scheduled with the client's leadership, management, and technical stakeholders to discuss the security issues raised during the engagement and promote a more security-aware culture.

Expected Business Benefits

BlackBerry Security Services CA engagements help organizations take a proactive, prevention-based approach to cyber risk management. Past breaches can be identified, and their causes assessed to prevent a recurrence. Breaches in progress can be traced, terminated, and remediated. Confidence in the organization's security posture can be restored. Typical benefits include:

- **Rapid Response:** The wait time for a traditional consulting firm to assess a client's environment or respond to a potential breach can stretch into weeks, allowing damage to spread while driving up the costs of recovery and cleanup. BlackBerry Security Services CA consultants are available at a moment's notice to deliver consistent, best-in-class services anywhere in the world.

BlackBerry Security Services CA engagements help organizations take a proactive, prevention-based approach to cyber risk management.

- **Rapid Results:** BlackBerry Security Services CA teams utilize best-practice, field-proven methodologies that leverage AI to produce results quickly.
- **Comprehensive Analysis:** BlackBerry's proprietary tools support network-wide forensic analysis and leverage IOCs from thousands of previous consulting engagements.
- **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 CA consultants provides internal teams with invaluable opportunities for education and skill-building.
- **Proactive Risk Reduction:** Organizations learn from previous breaches how to reduce their risk exposure and prevent future incidents.

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.

BB20-0407 | 200710