BlackBerry

DATASHEET

BlackBerry Cybersecurity Consulting:

Security Assessments

The Challenge:

Ensure your systems are secure with threat detection, penetration testing, vulnerability and red team assessment services.

The Solution

Successful businesses are built on trust. Trust in products and services, trust in and among your employees, and trust by customers in your brand. Cyber-attacks take advantage of this trust to access and disrupt your business. To protect the trust in your organization, you need a security partner that can help you respond, identify, and prepare for ongoing cybersecurity threats.

Global Leader in Security

The world's leading organizations as well as national government agencies rely on BlackBerry products and services to secure their mission critical operations. BlackBerry has the in-depth knowledge and investigative experience to help organizations identify and mitigate today's increasingly sophisticated threats. In verticals prone to attack, such as Banking, Insurance, Healthcare, and Transportation, BlackBerry security teams provide the expertise and guidance to defeat persistent, well-funded attacks. Our customers include 100% of the F100 Commercial Banks, 10 of the 10 largest law firms, and 16 of the G20 governments.

Security Assessments

We are able to offer a range of security assessments based on your needs and situation. Our highly accredited consultants will assess vulnerabilities in any infrastructure, device or configuration, including SCADA and CNI. We also provide physical security assessments, which include the use of social engineering techniques.

Threat Intelligence

We also offer an extended level of assessment that will consider the real life threats to any organization based on industry and strategic factors, building up a customized consideration of what threat actors present the greatest risks to your organization. This can also include the management of 3rd party ecosystem.

FIPS VALIDATED 140-2

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

CHECK
IT Health Check Service

Bundesamt
für Sicherheit in der
Informationstechnik

ISO 9001:2008
REGISTERED FIRM

CESG Check IT Health Check

We will carry out the assessment under the terms of CHECK as defined by CESG, inline with HMG standards. This will provide assurance that you can operate at a level of security that is suitable for handling sensitive information. Our testers are SC and DV cleared through GCHQ and can test IL data up to IL6 = TOP SECRET. Testing would be carried out by a CHECK Team Leader.

External IT Health Check

Testing will be performed in a 'Black box' method with no information about the services or servers provided to the test team; only confirmation of the external IP Addresses are provided. This method most closely replicates threats to the organization from a malicious attacker, who would have the same information as the test team.

Internal IT Health Check

Testing internal systems will determine the level of threat to an organisation that a malicious attacker, an employee or contractor, who has gained access to internal systems, may pose to the systems and data. We will examine the security of all server's OS, applications, wireless security, segregation of restricted data, VLAN and firewall rulesets and physical security. Testing will be onsite and will be partial 'white box', where relevant information is given. Testing is designed to cause no interference to normal network operation.

Wireless Penetration Testing

A wireless penetration test will examine security of all nominated wireless points and check for data leakage and security level. This will test the reliability of the organization's wireless network and prevent an attack.

Web Application Penetration Testing

A full test on the nominated website including OWASP most common vulnerabilities. A web application test employs different software testing techniques to find “security bugs” in server/client applications of the organization from the Internet. The outcome of this web application testing is for BlackBerry Cybersecurity Consulting to provide assurance that the organization's web presence is protected from penetration and compromise from intruders.

Mobile Device Penetration Testing

Penetration testing of mobile phones (BlackBerry, Android, iPhone), tablets and laptops. Testing will consist of attempted access to a mobile device without authentication devices or provided passwords. A second phase of testing will also be undertaken with full authentication provided allowing the tester's access to the device as an employee would have. As a CHECK approved company we will advise the client on best practice in configuring all mobile devices to Government standards suitable for connection to different environments including protectively marked.

Social Engineering & Physical Security

Environment and people vulnerabilities can be a larger threat than network and IT vulnerabilities. Social engineering is the Art/Science of manipulating someone in order to bypass security measures and tools. This test will identify any vulnerabilities in an organization's staff and physical access to the organization's' building.

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. BlackBerry is a GDPR compliant, ISO22301 & ISO27001 certified company.

Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The company trades under the ticker symbols “BB” on the Toronto Stock Exchange and “BB” on the New York Stock Exchange.

For more information, visit **blackberry.com/cybersecurity**