HOW CYBER THREAT INTELLIGENCE HELPS BUSINESSES ACHIEVE CYBER RESILIENCE

A cyber resilient organization can protect and defend its infrastructure from a growing range of cyberthreats to ensure uninterrupted operations and secure applications and data. True cyber resilience demands more than effective threat detection and response—businesses also need actionable cyber threat intelligence (CTI) to support informed actions, decisions, and strategies. Comprehensive CTI includes three kinds of information:

Strategic threat intelligence helps security and leadership teams stay aware of threat actors' changing trends and motives.

Operational threat intelligence helps ensure security teams understand tactics, techniques, and procedures (TTPs) of specific threat actors and how they may impact the organization.

Tactical threat intelligence includes specific indicators of compromise (IOCs) to help security teams recognize and stop active threats.

Robust and timely CTI enables organizations to:

1 STAY AHEAD OF THE LATEST THREAT GROUPS AND ACTIVITIES

Failing to understand threat actors' motives and targets as well as attack vectors can create blind spots that lead to vulnerabilities and exposure. CTI empowers your organization to understand how potential threats are related to the global threat landscape, which can include changing geopolitical and economic environments, as well as dynamic risks associated with your industry, operational footprint, and even whether you publicly support a social cause or activist movement.

2 OPERATIONALIZE INTELLIGENCE FOR IMMEDIATE ACTION

When threats arise, security teams must act quickly. High-quality CTI helps teams deepen their understanding of threat goals, attack vectors, and patterns so they can map intelligence to the unique conditions of their infrastructure for rapid and proactive threat prevention, detection, and response.

3 OPTIMIZE RESPONSE AUTOMATION AND VERIFICATION

Understanding emerging and historical tactics, techniques, and procedures (TTPs) helps security teams verify their presence and speed response automation. CTI delivers valuable TTP data that helps teams quickly identify, prioritize, and remediate incidents and automatically block the threats in the future.

4 ACCESS TIMELY, RELEVANT, AND CONTEXTUAL INSIGHTS AND ANALYSIS

In addition to supporting immediate action, CTI delivers relevant insights that empower teams to understand and apply relevant threat information within their environment and craft the most efficient and effective security strategies.

5 HUNT FOR THREATS WITH SPEED AND PRECISION

As threats and threat actors evolve, security teams need accurate, up-to-the-minute information about TTPs and IOCs as well as actionable strategies to prevent, detect, and resolve them. High-quality CTI delivers meaningful guidance to support effective threat hunting and eradication strategies.

6 CORRELATE EVENTS

The attack surface now includes remote and mobile workers, cloud and hybrid environments, Internet of Things (IoT), and operational technology (OT). CTI enables security teams to identify and investigate potential connections among seemingly unrelated events across an expanding infrastructure.

7 ASSESS SECURITY POSTURE

Evaluating enterprise-wide security posture requires understanding how the vast range of potential threats may attempt to enter the organization. Comprehensive CTI helps security teams understand the threat landscape to accurately assess risk and secure operations.

8 IMPROVE STAKEHOLDER REPORTING AND ROADMAP DEVELOPMENT

Without CTI, business leaders may not understand the value of security activities or how they support the organization's goals. As a result, organizations may misallocate funds and resources or unintentionally create security gaps. CTI helps align all stakeholders around a shared security mission.

CTI is essential knowledge for strengthening cyber resilience. If your organization is ready to be proactive, CTI will empower your teams to reduce successful cyberattacks, improve overall threat response, and increase performance and ROI across the enterprise.

CylancelNTELLIGENCE™ helps organizations avoid sophisticated cyberattacks by delivering contextual threat intelligence designed to prevent, hunt, and respond to dynamic threats. CylancelNTELLIGENCE synthesizes multiple data sources including early CTI signals, live threat hunting, and in-house telemetry gathered from the BlackBerry® portfolio of Cylance® AI solutions. With access to actionable, expertly crafted threat intelligence, organizations can better understand their adversaries, motivations, and tactics to identify gaps, prioritize investments, and create a more cyber-resilient organization.

To deliver the highest quality CTI, BlackBerry employs an international team of experts, offering 24x7x365 global coverage, with extensive experience in the threat intelligence lifecycle to collect, process, analyze, and distribute highly contextual and actionable threat intelligence.

BlackBerry is also a member of the Joint Cyber Defense Collaborative (JCDC), established by the Cybersecurity and Infrastructure Security Agency (CISA), working alongside a community of public and private organizations helping to proactively gather, analyze, and share actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response worldwide.

For more information or to arrange a demo, visit our website.

BlackBerry. Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 215M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

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

88023 | 230502