BlackBerry

Intelligent Security. Everywhere.

Summary Brief

BlackBerry MITRE ATT&CK APT29 Evaluation

BlackBerry Excels Against Advanced Attack Techniques

What Is MITRE ATT&CK?

The MITRE ATT&CK® framework is a global knowledge base of threat actors' tactics and techniques drawn from real-world cyber attacks. As such, it highlights potential attack vectors and uniformly describes the how and why of a threat actor's actions. MITRE provides a common knowledge base and verbiage for describing attacks, ultimately benefiting end-users by organizing complex information into an understandable and actionable format.

Cybersecurity vendors likewise benefit by testing their solutions against the framework and measuring the effectiveness of their tools against known attack strategies and adversarial behaviors. MITRE ATT&CK testing is transparent and the evaluation results are available to vendors and end-users alike, without commentary or bias.

The MITRE ATT&CK evaluations are not a competitive system used for selecting winners in the cybersecurity industry. It does not pit solutions against each other, quantitatively rate products, or score a vendor's performance. Test results are recorded in a success matrix that offers readers insight into how each vendor fared against each threat technique or tactic. This report contains BlackBerry's analysis of the MITRE ATT&CK APT29 evaluation data, as MITRE offers no interpretation of test results.

BlackBerry Excels in the APT29 Evaluation

BlackBerry recently participated in the MITRE ATT&CK APT29 evaluation. BlackBerry® Protect, BlackBerry® Optics, and BlackBerry® Guard were tested against the attack strategies of APT29, a threat group reportedly tied to the Russian government. The APT29 group is known for carrying out high-profile attacks, including the United States Democratic National Committee breach of 2015.

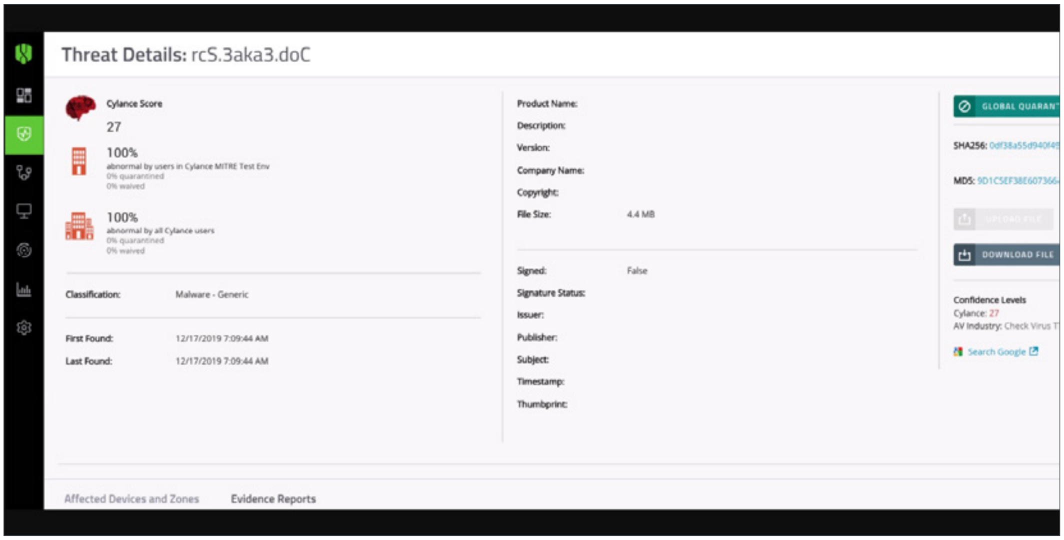
BlackBerry® solutions performed well throughout these tests, surpassing our own high expectations. MITRE employee and ATT&CK Evaluations lead, Frank Duff, said, "Taken as a whole, the results indicate that the participating vendors are beginning to understand how to detect the advanced techniques used by groups like APT29, and develop products that provide actionable data in response for their users."

The Power of Prevention

The MITRE ATT&CK APT29 evaluation did not include steps to measure a solution's ability to prevent an attack. Nevertheless, BlackBerry Protect did detect the malicious nature of the infected file dropped during the tests. Had the evaluation represented a real-world attack, BlackBerry Protect would have stopped it as soon as the malicious file arrived on a protected system.

BlackBerry. Protect

As MITRE mentions on their website, "Also, it should be noted that (BlackBerry) Cylance's platform would have prevented the attacks that were conducted at many points within the kill chain. From quarantining binaries to preventing successful exploits and scripts from running, however the platform was configured to allow these attacks to occur."



Threat Details: rcS.3aka3.doC

Cylance Score
27

100%
abnormal by users in Cylance MITRE Test Env
0% quarantined
0% waived

100%
abnormal by all Cylance users
0% quarantined
0% waived

Classification: Malware - Generic

First Found: 12/17/2019 7:09:44 AM
Last Found: 12/17/2019 7:09:44 AM

Product Name:
Description:
Version:
Company Name:
Copyright:
File Size: 4.4 MB

Signed: False
Signature Status:
Issuer:
Publisher:
Subject:
Timestamp:
Thumbprint:

SHA256: 0df38a55d940f49

MD5: 9D1C5EF38E607366

Confidence Levels
Cylance: 27
AV Industry: Check Virus T

Figure 1. BlackBerry Protect detects the introduction of the malicious file before it executes.

BlackBerry Optics automatically detected the vast majority of attacker techniques and tactics during the evaluation. The detection logic in BlackBerry Optics can be easily extended to alert on tactics and techniques where BlackBerry solutions had the telemetry to observe an occurrence but did not automatically alert. This flexibility is not limited to MITRE ATT&CK tactics and techniques. Any endpoint telemetry can be converted into an automatic alert, allowing for rapid product customization.

Letting analysts customize and automate repetitive or time-consuming security tasks reduces employee workload without damaging the security posture. This increased efficiency allows security engineers more time to focus their attention on long-term strategies or address critical issues as they arise.

BlackBerry. Optics

Superior Threat Visibility

BlackBerry Optics offered visibility into all but one of the primary steps of the attack evaluation. Each evaluation step also contained one or more attack sub steps. Data captured by MITRE highlighted BlackBerry detections for the vast majority of evaluation sub steps.

BlackBerry Optics offered visibility into all but one of the primary steps of the attack evaluation. Each evaluation step also contained one or more attack sub steps.

The BlackBerry Optics endpoint detection and response (EDR) solution revealed attacks utilizing or modifying:

- PowerShell script block text and PowerShell interpreter payloads
- WMI hooks, consumers, and filters
- Automated Windows® event log parsing and analysis
- DNS requests and resolutions
- Static portable executable parsing and analysis

BlackBerry Optics increases visibility by deploying mathematical threat detection models directly on the endpoint and storing threat data locally. With BlackBerry Optics, analysts can quickly search for files, executables, hash values, and other indicators of compromise

(IOCs) across network endpoints to uncover hidden threats. Protected endpoints can also detect and react to suspicious behavior without encountering the communication delays suffered by cloud-based EDRs.

The new sensors released in BlackBerry Optics v2.4 proved to be a critical component of BlackBerry's success in this evaluation.

The new sensors improve:

- Registry introspection
- DNS visibility
- Windows logon event visibility
- RFC 1918 address space visibility
- Enhanced WMI introspection via Windows API
- Enhanced PowerShell introspection via Windows API

Detection Breadth

BlackBerry solutions demonstrated the advantages of leveraging AI for threat detection throughout the evaluation. This can be seen in Figure 2 (higher is better) where BlackBerry removed the MSSP aspect of the testing to eliminate human influence. BlackBerry solutions seek to minimize the costs associated with human intervention, including avoidable errors, slower response times, and bias-related mistakes. While manual investigations and analysis will always be required for security teams, excluding the MSSP-based detections shows how BlackBerry's AI-driven product performs on its own:

As MITRE mentions on their website, "Also, it should be noted that (BlackBerry) Cylance's platform would have prevented the attacks that were conducted at many points within the kill chain. From quarantining binaries to preventing successful exploits and scripts from running, however the platform was configured to allow these attacks to occur."

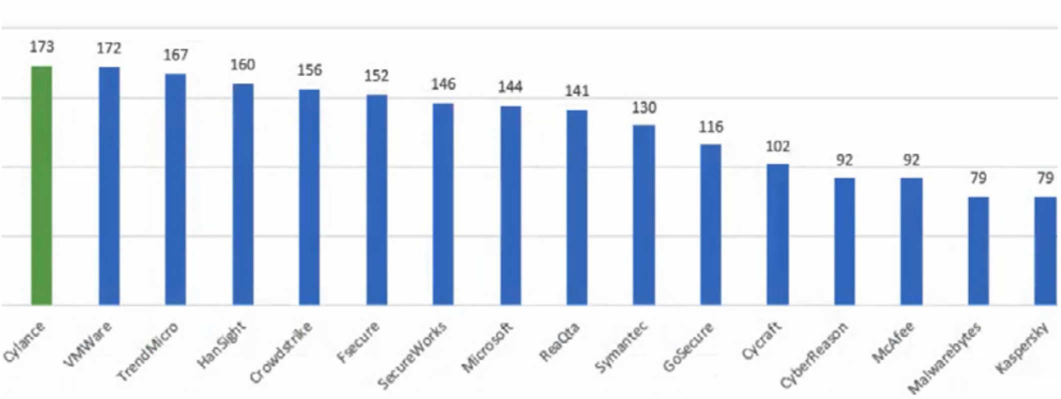
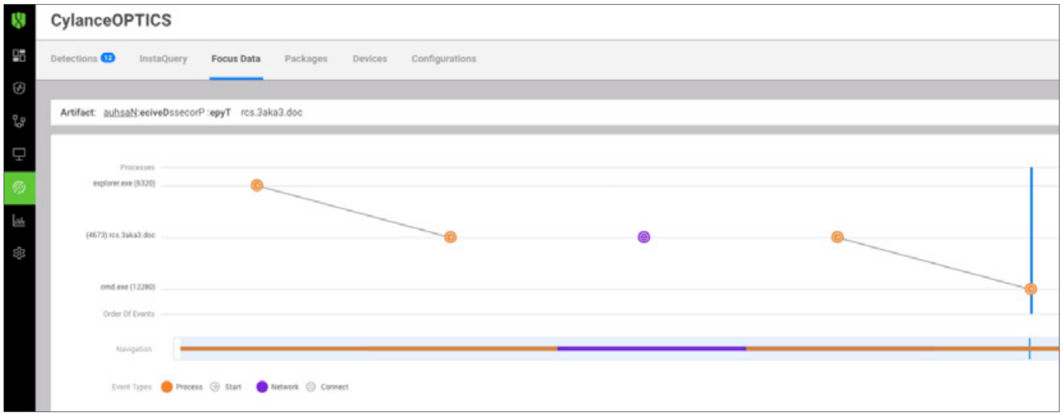


Figure 2. BlackBerry (Cylance) AI-driven threat detections.

The BlackBerry Protect AI-driven prevention solution scored several detections on dangerous files and general exploitation attempts. BlackBerry Optics aided BlackBerry Protect by detecting script events while also providing additional threat detection rules.

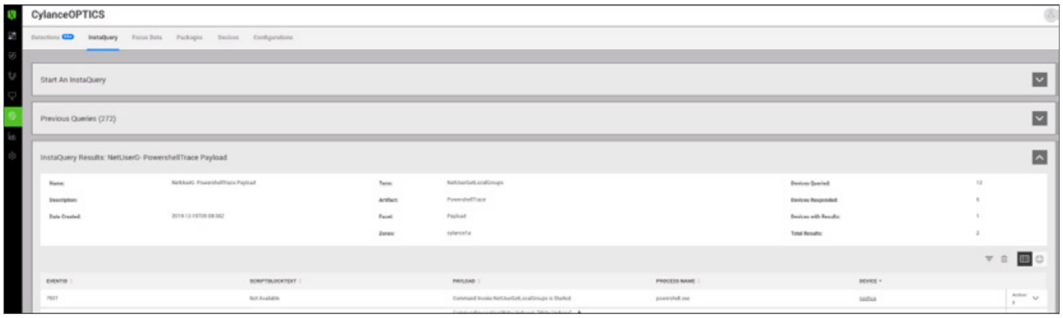
BlackBerry Optics presents focus data (a chain of related information starting with the first detected event) in three accessible Focus View layouts. Focus View is not part of the automated or AI-driven capabilities of BlackBerry Optics, but assists analysts by collecting and organizing critical threat information as seen in Figure 3. It does this by recreating the events associated with the detection and providing contextual details, including device, description, type, and date, and the relationship between each event in the trail. This allows a security analyst to easily identify and address security deficiencies and better overall security posture.



Artifact: auhsaN:eciveDssecorP :epyT rcs.3aka3.doc

Figure 3. BlackBerry Optics Focus View provides a bread-crumb trail of critical events.

The BlackBerry Guard subscription-based managed detection and response offering used features of BlackBerry Optics like InstaQuery in Figure 4 for threat hunting during the evaluation. The InstaQuery tool allows admins to quickly search for IOCs, suspicious activity, or other endpoint-related information throughout the environment. This offers security analysts simple, instant access to forensically relevant data.



InstaQuery Results: NetUserG- PowershellTrace Payload

Name: NetUserG- PowershellTrace Payload
Description:
Date Created: [illegible]
Term: NetUserGetLocalGroups
Artifact: PowershellTrace
Facet: Payload
Zones: [illegible]
Devices Queried: 12
Devices Responded: [illegible]
Devices with Results: 1
Total Results: 2

Figure 4. BlackBerry Optics InstaQuery provides an instantaneous telemetry detection.

Where BlackBerry products did not natively have telemetry for particular tactics or techniques, BlackBerry Guard analysts used the scripting capabilities built into BlackBerry Optics to retrieve and analyze raw forensic artifacts from the target systems.

Context Mapping

Understanding the context of an attack is key for performing successful remediation. The APT29 test contained 57 different tactics, techniques, and procedures. BlackBerry Optics had direct mapping to many of them, meaning no additional manual configuration was required for detections to occur. Unmapped techniques are fully addressable by modifying rulesets within BlackBerry Optics. In fact, BlackBerry verified the effectiveness of crafting specific BlackBerry Optics ruleset while working with other frameworks in preparation for this evaluation. BlackBerry Optics scored well in the evaluation without any manual configurations to assist its technique detection capabilities, as seen in Figure 5 (higher is better).

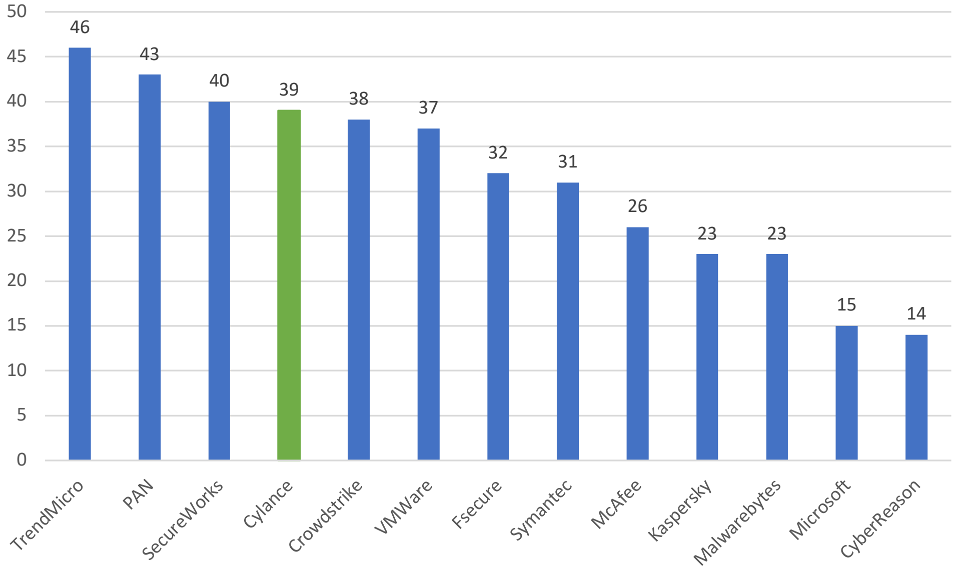


Figure 5. BlackBerry (Cylance) detects multiple APT29 tactics, techniques, and procedures through contextual analysis.

BlackBerry Optics uses an automated context analysis engine (CAE) to monitor and correlate suspicious endpoint events in near real time. The CAE allows analysts to observe and respond to events manually or create automated response actions based on specific rules. Automated response actions are initiated from the endpoint, eliminating the latency encountered by cloud-based or remotely managed solutions.

Conclusion

BlackBerry solutions performed extraordinarily well in terms of number of detections, far surpassing traditional EDR players. The BlackBerry Optics 2.4 sensors performed particularly well during this evaluation, proving its ability to meet market demand for effective, automated EDR. The MITRE ATT&CK APT29 evaluation clearly demonstrated that BlackBerry solutions protect systems from attack strategies used by world-class threat actors. BlackBerry solutions' mapping to threat techniques and tactics is robust and provides a balanced approach between automation and manual interaction that is effective.

For full results of the evaluation, please visit the MITRE page. MITRE does not offer interpretation or analysis of results, but BlackBerry is happy to discuss our performance and answer any questions. Please contact us with your inquiries.

About BlackBerry

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 150M cars on the road today. 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 management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

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

BlackBerry

Intelligent Security. Everywhere.

CONTACT US