SOLUTION BRIEF

AttackIQ-CrowdStrike Falcon Integration

Continuous Security Validation Capability for CrowdStrike Falcon

The Challenge

Unifying endpoint capabilities of next-generation anti-virus (Falcon Prevent), Endpoint Detection and Response (Falcon Insight), Managed Threat hunting (Falcon Overwatch), Security Hygiene (Falcon Discovery), and Cyber Threat Intelligence (Falcon Intelligence) all via the CrowdStrike Falcon Platform offers tremendous benefits to defend against unwanted attacker behavior. By combining together multiple defensive capabilities into a light-weight, cloud-managed endpoint across your infrastructure, your ability to thwart attackers improves greatly. But the effectiveness of unified data and alerts depends upon how the underlying technologies are configured. Optimal policy configuration and enforcement across all Falcon endpoints have traditionally been difficult to validate and measure, leaving your infrastructure in an unknown, and potentially vulnerable, state.

With AttackIQ, you can ensure the optimal efficacy of CrowdStrike Falcon and the current state of all Falcon endpoint configurations across your entire footprint. AttackIQ continuously verifies the proper configuration and safely emulates adversarial behavioral throughout your production environment to provide the opportunity for proper tuning and configuration before an attack occurs. Results from AttackIQ will help you determine how best to optimize the configuration of your CrowdStrike Falcon endpoints.

AttackIQ Platform

AttackIQ, the leading independent provider of continuous security validation, enables enterprise security teams to test and measure the effectiveness of their security capabilities. The number of security controls in the enterprise is growing rapidly, yet there hasn't been an automated way to test the efficacy of these controls. In order to get the most out of your security investment, you need the ability to continuously measure and validate that your controls are working as expected – and that they're arresting the latest attacker tactics, techniques, and procedures (TTPs). AttackIQ provides a powerful platform for configuration validation and attack emulation in a production environment without impacting your operations.

CrowdStrike Falcon Platform

CrowdStrike Falcon is purpose-built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks — including malware and much more. Today's sophisticated attackers are going "beyond malware" to breach organizations, increasingly relying on exploits, zero days, and hard-to-detect methods such as credential theft and tools that are already part of the victim's environment or operating system, such as PowerShell. CrowdStrike Falcon responds to those challenges with a powerful yet lightweight solution that unifies next-generation antivirus (NGAV), endpoint detection and response (EDR), managed threat hunting capabilities, and security hygiene — all contained in a tiny, single, lightweight sensor that is cloud-managed and delivered.

Key Benefits of the Integration

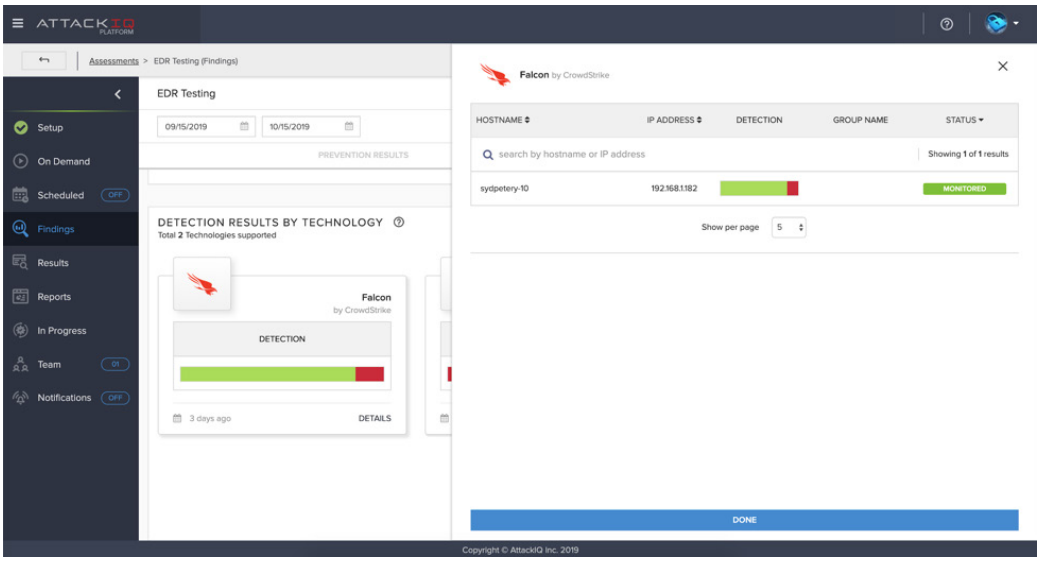
Ensure Crowdstrike Falcon is configured correctly and optimized to detect the latest threats.

Emulate real-world attacker behavior safely against Falcon endpoints.

CrowdStrike Falcon Platform and AttackIQ Platform Integration

AttackIQ supports integration with CrowdStrike to provide confidence via verifiable evidence in your Falcon endpoint security controls. By using the AttackIQ CrowdStrike Falcon integration, you will be able to verify proper configuration as well as measure, validate, and optimize core capabilities. Emulated adversarial behavior will be safely run against your infrastructure and fed back to your security analysts and IT teams. Based on testing results, your team can make data-driven decisions to determine how best to address any protection failures, detection gaps, or misconfigurations. AttackIQ extends the powerful capabilities of CrowdStrike Falcon by delivering impactful insight that helps security teams get the most out of their security investments. Combining

CrowdStrike Falcon with AttackIQ's award-winning continuous security validation platform allows customers to efficiently comply with regulations, secure their endpoints, and optimize the performance of their controls.



The integration showcases the real-time efficacy of a customer's CrowdStrike configuration based upon what AttackIQ detected from its adversarial emulations. Customers use this data to tune CrowdStrike for increasingly robust efficacy.

Use case #1: Validate prevention and detection capabilities of Falcon against complex attacks

Challenge: Security teams need to consistently prove the value of their security investments to ensure that they're reducing enterprise risk. Finding a credible, independent source to prove that a set of core protection capabilities demonstrably exist is an issue enterprise security leaders face.

Solution: AttackIQ enables you to create a repeatable CrowdStrike Falcon assessment template that is comprised of specific attack scenarios that can exercise Falcon agents and prove relevant protection capabilities to reduce risk. CrowdStrike Falcon assessments can be used to repeatedly and consistently prove to management, leadership, and other business units the existing capabilities given the security investment in CrowdStrike Falcon.

Use case #2: Identify and prove coverage of Falcon against the MITRE ATT&CK Framework

Challenge: MITRE's ATT&CK Framework provides an extensive list of capabilities and techniques that attackers have used in various real-world attacks. The challenge has been how to efficiently and effectively emulate the attacks in a repeatable, accurate manner in order to see what security controls like CrowdStrike Falcon provide in terms of coverage.

Solution: AttackIQ emulates—in a safe, controlled manner—adversarial behavior so as to exercise, validate, and measure your endpoint security controls. AttackIQ has fully operationalized the MITRE ATT&CK Framework into the Platform, enabling you to select and run specific assessments to exercise Falcon's security controls and provide efficacy metrics for prevention and detection against specific adversarial TTPs and attacker groups.

About AttackIQ

AttackIQ is the leading independent provider of continuous security validation and has built the first platform that enables organizations to measure and validate the effectiveness of their security program.

Leveraging the MITRE ATT&CK framework, AttackIQ provides organizations with evidence to prove current capabilities and also determine the highest probability risk exposures and gaps in their defensive strategy. Empowered by data, organizations can now make data-driven decisions to minimize the risk to their business.

About CrowdStrike

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene, vulnerability assessment, and a 24/7 managed hunting service — all delivered via a single lightweight agent. Find out more at www.CrowdStrike.com

AttackIQ Headquarters | 2901 Tasman Drive, Suite 112 | Santa Clara, CA 95054 | +1 (888) 588-9116 | crowdstrike-alliance@attackiq.com