Solution Brief

AttackIQ and Qualys

Aligning threat and risk management in a united security strategy.

Problem

Threats are outpacing cyberdefense operations and the problem is getting worse as the world expands its infrastructure and presence online. Organizations lack a systems-based, holistic approach to managing security. Configuration management plagues organizations and security controls fail constantly, with EDRs only performing at 39% effectiveness against top-tier threats. Despites decades of improvement in technology, organizations still cannot measure and prove consistent real security effectiveness.

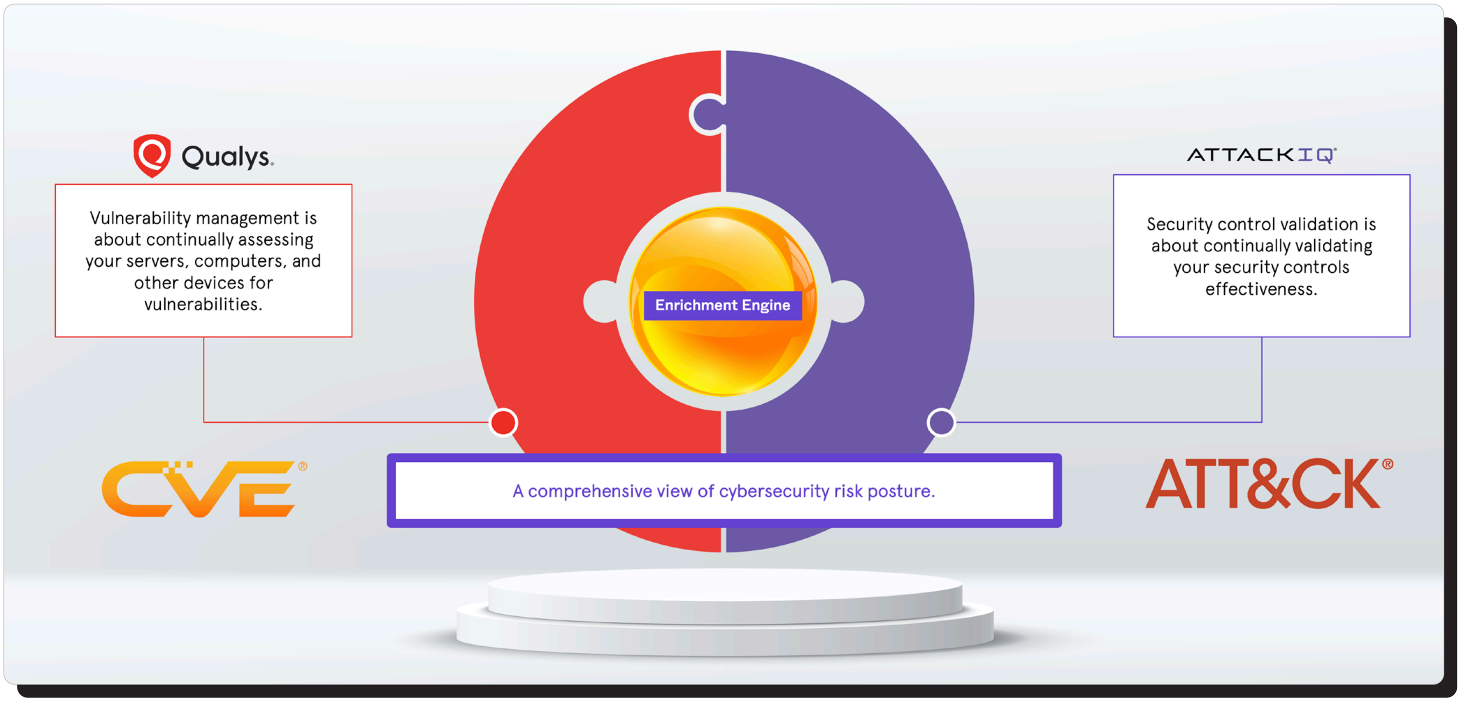
Impact

Executives lack granular, specific data required to make risk-informed decisions about the effectiveness of security teams, technologies, and processes. Boards of Directors and executives require clear visibility about team and technology performance to ensure resilience against attacks, and today they lack it. Adversaries are winning an asymmetric war in cyberspace – and defenders are losing.

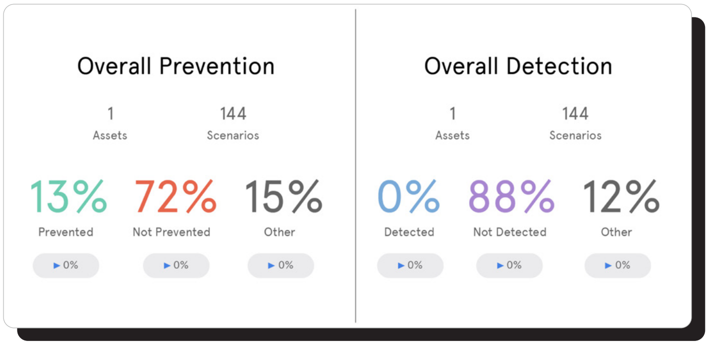
Joint Solution

To meet this challenge, Qualys and AttackIQ are converging in a new joint solution that combines two vital performance measurements:

1. Analyzing vulnerabilities and defending critical assets;
2. Measuring critical security control performance against real-world threats, aligned to MITRE ATT&CK.


Qualys.
Vulnerability management is about continually assessing your servers, computers, and other devices for vulnerabilities.
Enrichment Engine
ATTACKIQ
Security control validation is about continually validating your security controls effectiveness.
CVE
A comprehensive view of cybersecurity risk posture.
ATT&CK

Adopting a threat-informed defense:
The combination of Qualys and AttackIQ data provides a comprehensive portrait of the organization's overall risk and threat management posture. Security teams are measuring their critical security control performance against the adversary from initial vulnerabilities across the entire MITRE ATT&CK framework of known adversary tactics, techniques, and procedures. This is called a "threat-informed defense." Teams can now answer the question: are we ready for the next attack? As a result, teams suffer less burnout, save resources, and operate with improved confidence.



Overall Prevention

1 Assets | 144 Scenarios

13% Prevented | 72% Not Prevented | 15% Other

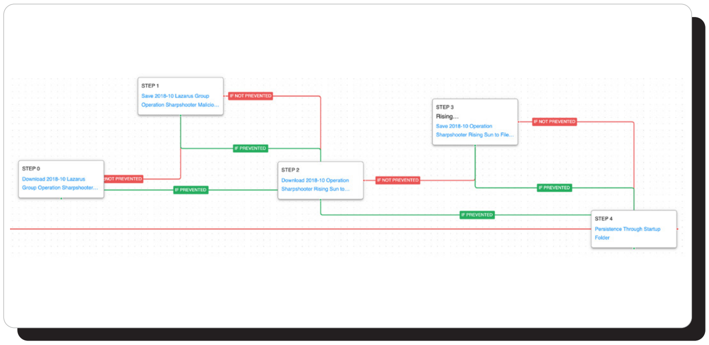
▶ 0% | ▶ 0% | ▶ 0%

Overall Detection

1 Assets | 144 Scenarios

0% Detected | 88% Not Detected | 12% Other

▶ 0% | ▶ 0% | ▶ 0%


STEP 1
Save 2018-10 Lazarus Group Operation Sharpshooter Malicio...
IF NOT PREVENTED
IF PREVENTED
STEP 3
Rising...
Save 2018-10 Operation Sharpshooter Rising Sun to File...
IF NOT PREVENTED
STEP 0
Download 2018-10 Lazarus Group Operation Sharpshooter...
NOT PREVENTED
IF PREVENTED
STEP 2
Download 2018-10 Operation Sharpshooter Rising Sun to...
IF NOT PREVENTED
IF PREVENTED
IF PREVENTED
STEP 4
Persistence Through Startup Folder

Combining Qualys and AttackIQ

Data-Driven Analysis for Real Security Outcomes

How does it work? Today Qualys customers use the Qualys platform to measure risk across vulnerabilities, assets, and groups of assets. The Qualys database generates insights from over 180 thousand vulnerabilities and a stream of threat sources to alert about potential attacks. This is half of the equation of aligning risk and threat management. The combination of Qualys's vulnerability management capabilities with AttackIQ's continuous security control testing process complete the circle. In the joint solution, teams operate from a single set of assets and a single list of top-tier threats, running AtackIQ assessments to generate real-time performance data to fix misconfigurations, improve team cohesion, and enhance decision-making. The resulting improvement in operational excellence leads to significant savings across the business as breaches decrease in impact and teams gain back valuable time.

The Joint Solution: A Data-driven Enrichment Engine
Qualys and AttackIQ are combining (1) Qualys's analysis of critical infrastructure vulnerabilities with (2) AttackIQ's analysis of the effectiveness of the controls that protect that infrastructure to provide a comprehensive cybersecurity strategy. Team can now test their security programs using a mix of atomic testing, comprehensive campaign emulations, and packet capture (PCAP) replay to validate internal and boundary control performance. AttackIQ's deep alignment with the MITRE ATT&CK framework and open API allows teams to tailor their testing against a range of controls, to include EDR, cloud security, DLP, next generation firewalls, micro-segmentation, antivirus, web application firewalls, and proxies. Armed with intelligence and research from organizations like MITRE ATT&CK and the Center for Threat-Informed Defense, the Qualys/AttackIQ joint solution helps breakdown silos between red and blue teams to adopt a purple team construct that significant improves internal coordination. Finally, teams use the joint solution's in-app Jupyter notebooks to aggregate, analyze, and present information from the Qualys/AttackIQ dataset in clear reports for the C-suite and the board, improving communication and confidence.

Qualys:

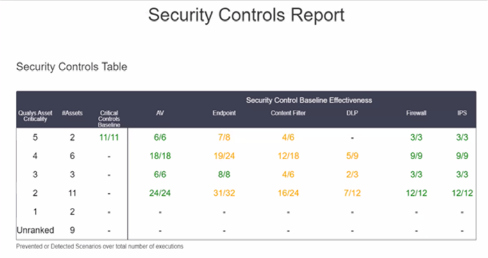
- Vulnerability Management
- CVE
- Asset Inventory
- Asset Criticality
- Application Inventory
- External Attack Surface Management

AttackIQ:

- Threat Intelligence / TTPs
- MITRE ATT&CK
- Testing Key Defense Technologies
- Security Control Performance Data
- Center for Threat-Informed Defense

Enrichment Engine Functions

- Displays security control performance metrics (AttackIQ) within the context of asset criticality (Qualys). Prioritization is one of the most important aspects for improving team performance and effectiveness. Combining Qualys's asset criticality analysis with AttackIQ's security control validation data gives teams a single portrait of their overall risk posture from the perspective of critical assets. You can then dive deeper into the analysis to examine the problem from different perspectives, to include the MITRE ATT&CK framework and the MITRE CVE framework.



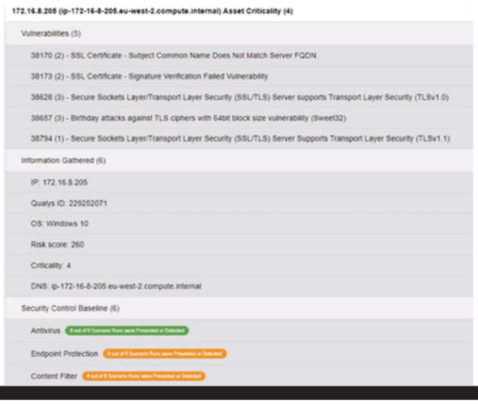
Security Controls Report

Security Controls Table

			Security Control Baseline Effectiveness					
Qualys Asset Criticality	#Assets	Critical Controls Baseline	AV	Endpoint	Content Filter	DLP	Firewall	IPS
5	2	11/11	6/6	7/8	4/6	-	3/3	3/3
4	6	-	18/18	19/24	12/18	5/9	9/9	9/9
3	3	-	6/6	8/8	4/6	2/3	3/3	3/3
2	11	-	24/24	31/32	16/24	7/12	12/12	12/12
1	2	-	-	-	-	-	-	-
Unranked	9	-	-	-	-	-	-	-

Prevented or Detected Scenarios over total number of executions

- *Organizes data on the basis of asset criticality, CVE, and ATT&CK-based metrics.* The joint solution provides a comprehensive picture of asset criticality, CVE, security control performance measurements. You can see how your organization will respond to the adversary from the point of entry at the vulnerability to your critical compensating controls' response. With a clear and comprehensive picture, teams can better allocate resources to defend the data that matters most.



172.16.8.205 (ip-172-16-8-205.eu-west-2.compute.internal) Asset Criticality (4)

Vulnerabilities (5)

38170 (2) - SSL Certificate - Subject Common Name Does Not Match Server FQDN

38173 (2) - SSL Certificate - Signature Verification Failed Vulnerability

38628 (3) - Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

38657 (3) - Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)

38794 (1) - Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

Information Gathered (6)

IP: 172.16.8.205

Qualys ID: 229252071

OS: Windows 10

Risk score: 260

Criticality: 4

DNS: ip-172-16-8-205.eu-west-2.compute.internal

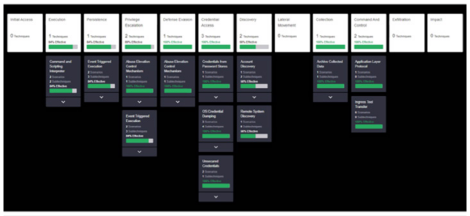
Security Control Baseline (6)

Antivirus 6 out of 6 Scenario Runs were Prevented or Detected

Endpoint Protection 6 out of 8 Scenario Runs were Prevented or Detected

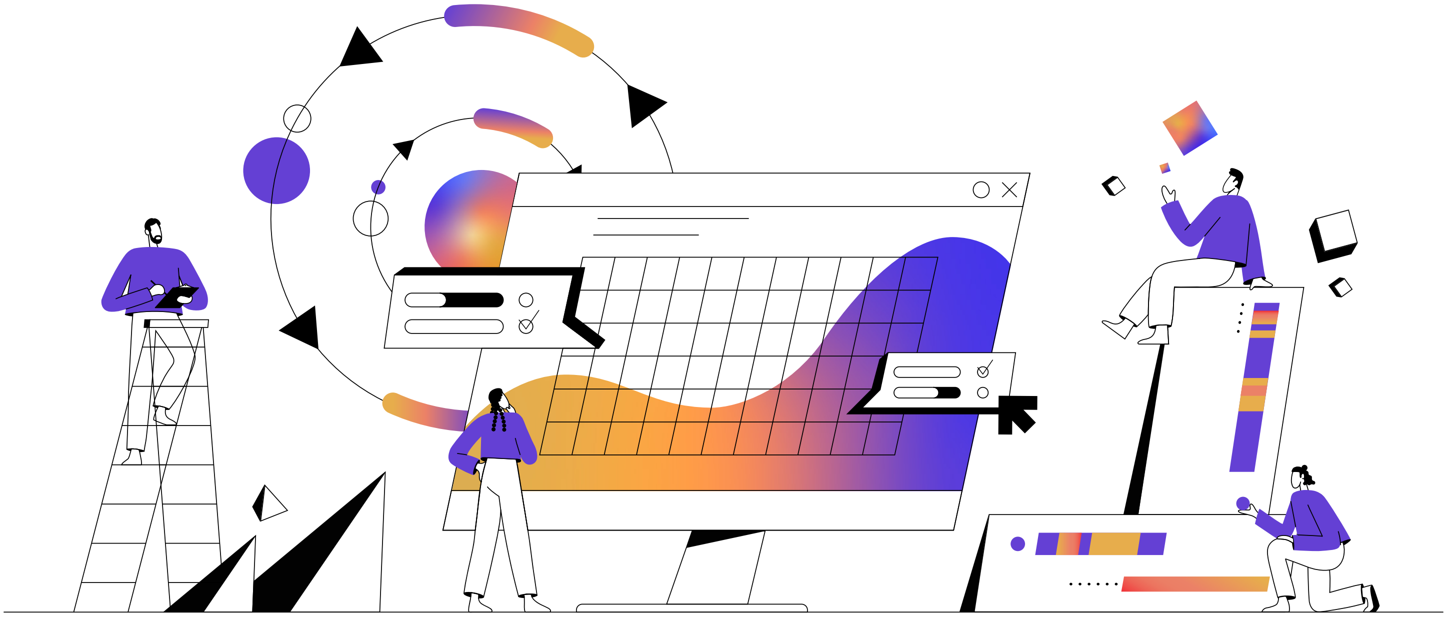
Content Filter 4 out of 8 Scenario Runs were Prevented or Detected

- *Provides a clear view of security control performance on the basis of MITRE ATT&CK tactics, techniques, and procedures.* Security leaders, the C-suite, and the board all want to know at any given moment how prepared they are for the adversary. MITRE ATT&CK-based reports provide a transformative, easy to consume, and clear picture of your security control effectiveness.



The evolution of cybersecurity operations.

The cybersecurity industry has made immense progress in improving the process of understanding assets and vulnerabilities. Now the industry is evolving through the practice of threat-informed defense to align risk and threat management. The joint Qualys/AttackIQ solution provides a comprehensive portrait of your security posture and total security effectiveness. You can see your vulnerability posture, see your security control effectiveness, and adopt a systems-based approach to operations. The joint solution helps teams prioritize vulnerabilities to patch while also measuring the security effectiveness of critical assets. With the combined data enrichment engine of the two organizations, security teams can continuously improve their performance. The whole organization knows what's working and what isn't, giving them a clear path to real cybersecurity and an overall increase in confidence.



ATTACKIQ®

U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Engenuity's Center for Threat Informed Defense

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.