Solution brief

IBM QRadar and Cisco Cloud Security Integration

With Umbrella, Enforcement and Investigate APIs, and Cisco Cloudlock

Application Highlights

- **Identify cloud and internet threats** in real time and prioritize attacks with the biggest potential impact.
- **Reduce the time** to detect, remediate and respond to advanced threats with context-rich cloud and internet analytics and threat intelligence.
- **Intelligently gather all threats** into a single pane of glass versus pivoting on disparate tools and interfaces.
- **Avoid alert fatigue** with the potential of missing alerts in the noise of event data.

Overview

As business transactions are pushed outside company walls, traditional security defenses to secure the perimeter are no longer effective. Users are now connecting from remote locations, and often without using a VPN. Branch offices are connecting directly to the internet, rather than backhauling traffic to the secure corporate network. This results in security teams having less visibility and control over their network than ever before.

Additionally, some enterprises have as many as 85 tools from many different vendors to address these security gaps. These disparate point solutions increase complexity and generate more security alerts than organizations can feasibly respond to with their limited resources. According to the Cisco 2017 Annual Cybersecurity Report, 44 percent of security alerts go entirely uninvestigated.

IBM and Cisco Security have teamed up to provide integrated solutions to address these challenges. The Cisco Cloud Security App integrates directly with the IBM QRadar Security Intelligence platform. This app leverages Cisco Umbrella, Investigate API, and Cisco Cloudlock to combine threat detection, cloud security, and advanced intelligence in a single dashboard.

When this app is installed in QRadar, multiple tabs are accessible, each providing critical security information visible on one console.

Key Capabilities

Single Console – multiple functions are available from the QRadar menu providing critical security information on one console.

Internet Threat Detection – the Umbrella tab provides visibility into internet activity across all locations, devices, and users. Views include the number of domains allowed and blocked by content category, number of events by identity, compromised users and devices, and various trend reports.

Cloud Infrastructure Security - Cloudlock is a Cloud Access Security Broker (CASB) and protects across users, data and apps in the cloud. The Cloudlock tab provides a live cloud incident feed, highlighting account compromises, data breaches, risky applications and advanced threats. This allows the SOC to triage and update incidents within QRadar. It also includes mapping and drill-down functionality to understand context.

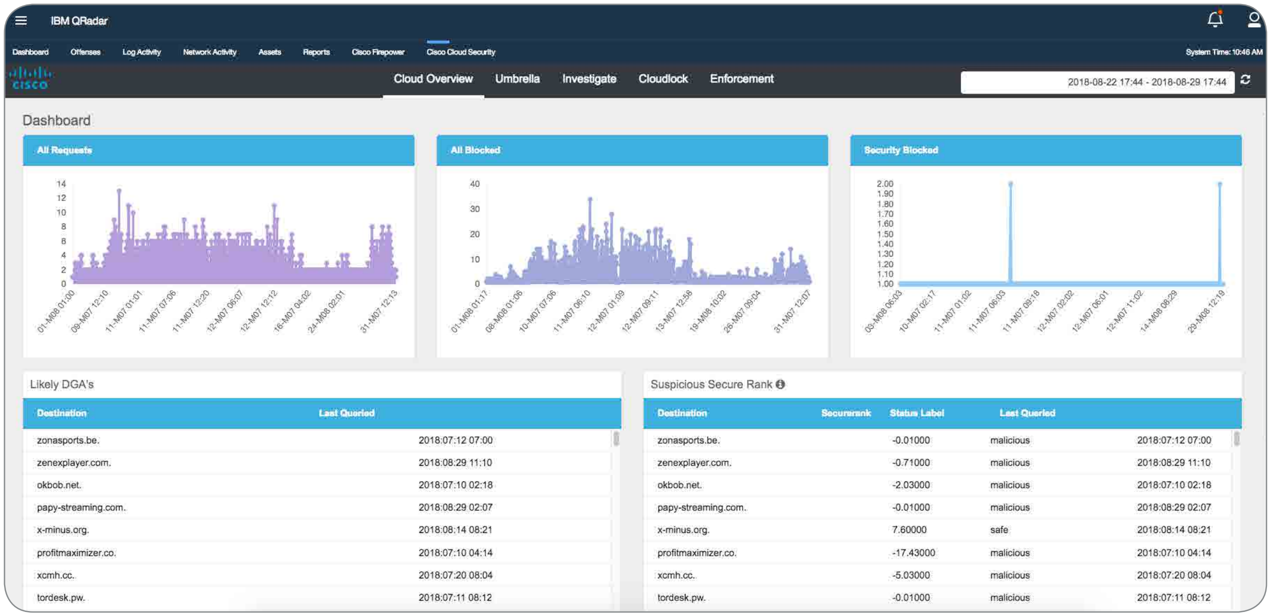
Advanced Contextual Intelligence - the Investigate tab provides threat insight beyond general offenses and alerts with the ability to drill down into domains, IPs and malware file hashes. This accelerates incident investigations with views of risk score, record data, malware samples, and other security features.

The Cloud Security App for QRadar enables a more efficient cross-team workflow while capturing, correlating and prioritizing events into a single pane of glass for faster threat analysis and remediation.

Fast Threat Detection and Mitigation

Security analysts are faced with the daunting task of detecting advanced threats, analyzing them to determine the severity, and conducting rapid incident responses. Many of these tasks are manual and labor intensive, causing missed threat indicators and delayed responses to the most severe events.

Cisco's Cloud Security App (Cisco Umbrella, Investigate, and Cisco Cloudlock) integrates with IBM QRadar, enabling security analysts to identify and mitigate internet and cloud threats faster and more effectively. This powerful app combines internet threat detection, cloud infrastructure security and advanced contextual intelligence in one unified solution.



Likely DGA's

Destination	Last Queried
zonasports.be.	2018:07:12 07:00
zenexplayer.com.	2018:08:29 11:10
okbob.net.	2018:07:10 02:18
papy-streaming.com.	2018:08:29 02:07
x-minus.org.	2018:08:14 08:21
profitmaximizer.co.	2018:07:10 04:14
xcmh.cc.	2018:07:20 08:04
tordesk.pw.	2018:07:11 08:12

Suspicious Secure Rank ℹ

Destination	Securerank	Status Label	Last Queried
zonasports.be.	-0.01000	malicious	2018:07:12 07:00
zenexplayer.com.	-0.71000	malicious	2018:08:29 11:10
okbob.net.	-2.03000	malicious	2018:07:10 02:18
papy-streaming.com.	-0.01000	malicious	2018:08:29 02:07
x-minus.org.	7.60000	safe	2018:08:14 08:21
profitmaximizer.co.	-17.43000	malicious	2018:07:10 04:14
xcmh.cc.	-5.03000	malicious	2018:07:20 08:04
tordesk.pw.	-0.01000	malicious	2018:07:11 08:12

The Cisco Security and IBM Security Advantage

The ongoing collaboration between Cisco Security and IBM Security helps organizations strengthen their security posture against increasingly sophisticated cyberattacks. Rather than working in silos, these two leading security providers are collaborating to build solutions and share threat information that will empower clients to act at extreme speed and scale to see a threat once - and protect everywhere.

Next Steps

The IBM QRadar and Cisco Cloud Security solution enables customers to rapidly detect, analyze, and remediate threats. This application enables customers to better protect their environments by reducing the time to detect and respond to advanced threats. With all this power in a single pane of glass, security analysts can eliminate redundant and tedious tasks for more effective security operations. This app is now available at no charge on the IBM Security App Exchange. For more information visit here.