illumio | IBM Security

SOLUTION BRIEF

Illumio + IBM Security QRadar XDR Integration for Accelerated Ransomware Containment

Preemptively limit an attacker's spread radius, detect threats in the environment faster, and stop ransomware from becoming a cyber disaster with automated containment

Lateral Attacks Evade Detection With Speed and Stealth

Most internal (east-west) networks are characterized by excessive lateral connectivity, and an over-reliance on firewalls, which were not designed to overcome the speed and stealth of modern, lateral attacks. Consequently, organizations struggle to employ firewall rules, at scale, that can preemptively contain an attack to one corner of the network, that can deny and rapidly analyze lateral movement attempts, and that can provide rapid, automated containment.

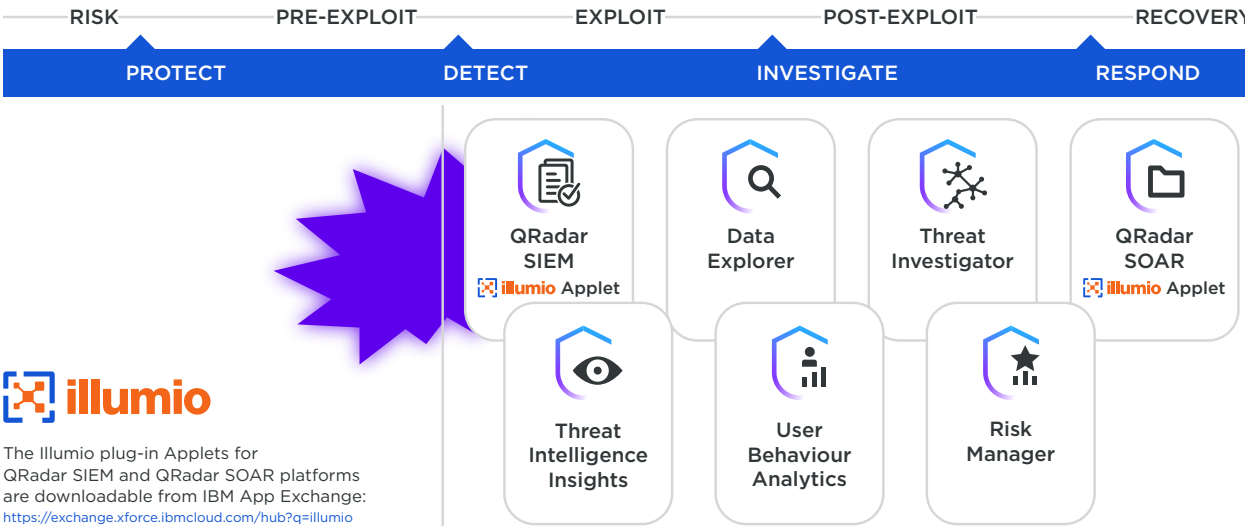
Fortunately, Zero Trust Segmentation solutions like Illumio Core were explicitly designed to address these challenges. When integrated with SIEM and SOAR platforms, the resulting solution delivers both the visibility and responsiveness needed to overcome the attacker's stealth and speed.

Illumio and QRadar XDR Open Architecture: A Perfect Match

The integration of Illumio Core with QRadar XDR (which includes both the IBM Security QRadar SIEM and IBM Security QRadar SOAR platforms) enables a workflow designed explicitly to eliminate the attacker's advantages:

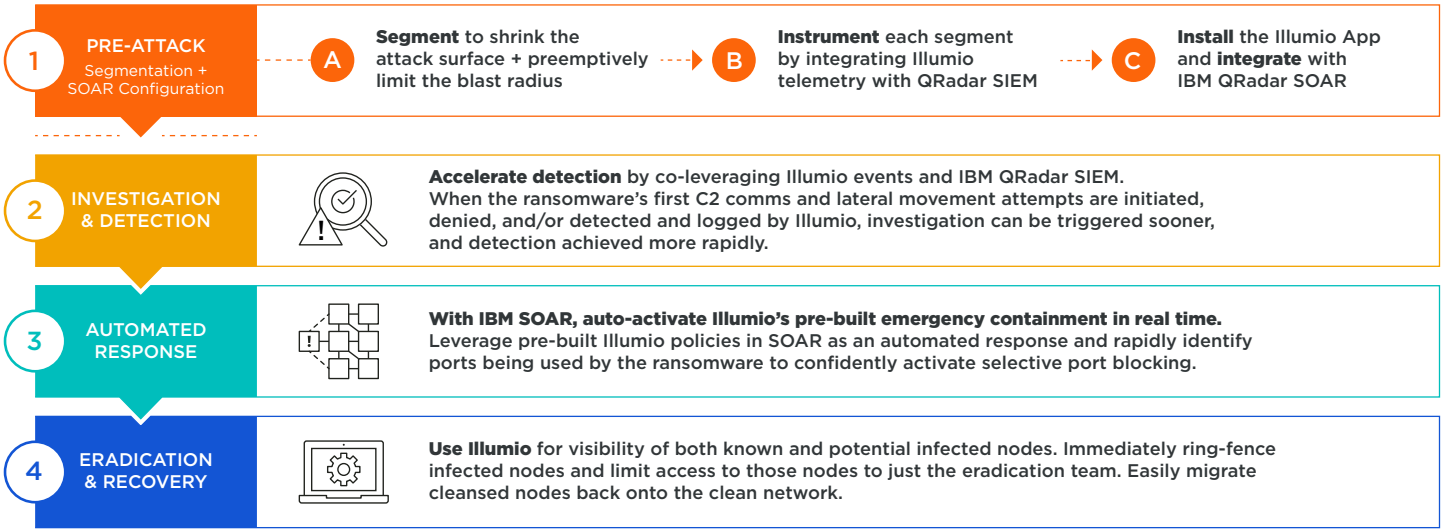
- Create preemptive containment barriers by segmenting and instrumenting the east-west network
- Accelerate detection when initial lateral movement attempts are initiated, denied and analyzed within the QRadar SIEM platform
- Auto-activate Illumio's emergency ransomware containment controls within the QRadar SOAR platform, to stop ransomware in its tracks

Illumio and QRadar XDR Integration: Pre- and Post-Exploit Defense



illumio

The Illumio plug-in Applets for QRadar SIEM and QRadar SOAR platforms are downloadable from IBM App Exchange: https://exchange.xforce.ibmcloud.com/hub?q=illumio



Illumio and QRadar XDR Joint Solution: How It Works

The integration of Illumio Core with QRadar XDR (which includes both the QRadar SIEM and QRadar SOAR platforms) enables a workflow that shifts the advantage from the attacker to the defender and is designed explicitly to eliminate the attacker's advantage of stealth and speed.

Step 1: Limit the impact of every future attacker, and instrument the attack surface to detect early indicators of compromise.
The first step of the workflow is complete before the next attacker shows up by using Illumio Core to preemptively segment the east-west network, eliminating excessive connectivity and creating containment barriers. These pre-attack containment barriers not only limit the potential spread of any subsequent intruder, but together with IBM helps defend against lateral movement.

Step 2: Enable earlier investigation and detection of lateral attacks.
When an intrusion does occur, initial lateral movement and communication attempts are blocked by Illumio and analyzed within the QRadar SIEM platform. This real-time visibility and analysis allows for earlier investigation and detection of ransomware and other lateral attacks.

Step 3: Automate response and rapid ransomware containment.
Having benefited from earlier detection, Illumio's integration with QRadar XDR enables earlier and more rapid, automated remediation. Specifically, within the QRadar SOAR platform, incident responders activate Illumio's emergency ransomware containment controls in real time, stopping ransomware in its tracks.

Step 4: Achieve faster eradication and recovery.
As a final step, Illumio facilitates safe eradication and migration of cleansed nodes back onto the clean network and helps accelerate the recovery process.

Illumio + IBM Security: Eliminate Threats

Stop lateral movement with automation and contextual insights.

DOWNLOAD
Illumio App for QRadar SIEM
Illumio App for QRadar SOAR

Visit: www.illumio.com/partners/tap/ibm-security or www.ibm.com/security

About Illumio

As the pioneer of Zero Trust Segmentation, Illumio prevents breaches from becoming cyber disasters. Gain real-time visibility and segmentation control to see your risks, isolate attacks and secure your data across hybrid clouds, data centers and endpoint devices.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to effectively manage risk and defend against emerging threats.