Case Study

Cyberint

Top IR group uses Argos Edge™ to deliver visibility amidst mayhem

Mapping out external risk exposure in record time while under attack, and gaining critical context for investigation and remediation

The Challenge: getting critical big-picture visibility fast

The Cyber Quick Reaction Force (CQRF) is a premiere agency of world-class incident responders, providing a wide array of cybersecurity services such as proactive security, adversarial security, quick response to cyber attacks, and forensic investigations post/while under advanced ransomware and other sophisticated attacks.

Tasked with creating a rich map of external exposure as fast as possible, CQRF's CTO was initially seeking to gain total visibility into exposed external-facing assets across clients' networks and enrich their intelligence picture with relevant threat intelligence.

The team was evaluating two separate solutions, one for attack surface management, and one for threat intelligence. During Cyberint's POV, they quickly realized the speed and degree of visibility as well as the quality of the actionable intelligence the solution delivered.

"With Argos Edge™ we cover clients' known and unknown assets 25% faster."

CTO, CQRF

Challenges

Obtaining extensive integrated visibility into clients' external risk exposure while they are under attack

Solution

Deployed Argos Edge™

Impact

- 25% faster asset coverage
- Uncovered and mitigated the most relevant external risks - some of which unbeknownst to the clients
- Improved ransomware investigations, which drastically improved negotiations and remediation

Autonomous discovery is a huge advantage

Harnessing Argos Edge™ autonomous discovery allowed the team to quickly uncover unmanaged assets, open ports, misconfigurations, and exposed interfaces (due to lack of policy and documentation) - on average, 25% faster, often uncovering exposed external assets the clients weren't aware of.

Invaluable intel while under attack

The group uncovered leaked credentials from during initial recon. Leveraging Argos Edge to monitor malware logs, dark commerce, and gauge threat actors' intent regarding imminent attacks.

"On one occasion, we found additional context regarding a RAT (Redline stealer) on the Cyberint data lake." says the group's CTO, "More often than not we'll find leaked customer credentials."

"Now we can cancel several subscriptions to intelligence databases because Argos Edge™ had all their intel and more."

A powerful weapon against ransomware

In cases of ransomware attacks the group harnesses continuous monitoring of deep and dark web channels such as instant apps, onion sites, various closed forums, and markets to see if information is offered for sale, making sure that it hasn't been leaked yet - this has a profound effect on the nature of the response and the success of negotiations.

"Cyberint perfectly complemented our proprietary tools," says the group's CTO "It simply checks all our boxes. Visibility, hyper-relevance, actionable insights at record speed. It is an incident responder power tool."

About Cyberint

Cyberint fuses threat intelligence with attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities and more, ensuring continuous external protection from cyber threats.

To learn more how Cyberint helps organizations uncover and mitigate their most relevant external risks earlier visit www.cyberint.com

Cyberint