Case Study

Cyberint

A government's cyber defense unit achieves real-time focused protection for critical assets

With near-zero false-positives, the team delivers real-time detection, swift remediation, and unparalleled security to its people and digital assets

The Challenge: getting critical big-picture visibility fast

The Cyber Defense unit is responsible for governmental leadership in cyber defense, running its SOC in the face of cyber threats, and delivering professional guidance and training in the field of cyber defense to all government ministries and auxiliary units.

Tasked with adding value to government offices in the realms of leaked credentials and other data as well as gathering intelligence to preemptively prepare and defend against various cyber-attacks against government digital assets, the unit's Cyber Defense Guidance Lead was concerned with the safety of his analysts.

"The covertness of Argos is what sparked my initial interest", says the unit's Guidance Lead. The Raw Intelligence module allows us to easily gain access to hyper-relevant and reliable intelligence originating in deep and dark sources, without compromising the safety of our employees and the integrity of our critical assets."

"With Argos, we caught a code uploaded erroneously to a paste-bin site in less than 30 mins from the moment it was uploaded."

Guidance Lead

Challenges

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

Solution

Deployed Argos Raw Intel

Impact

- Gained better visibility and protection of all external facing governmental digital assets such as domains, websites, and applications
- Uncovered and mitigated the most relevant external risks in record time
- Improved cybersecurity trainings for government employees through rich intelligence obtained in a covert way

Autonomous discovery is a huge advantage

Harnessing Argos Edge™ autonomous discovery allowed the team to gain visibility to vulnerable assets such as interfaces without 2FA, how-to guides for defacement of government assets, sourced from the deep and dark web, and more.

As part of the unit's responsibilities are secure development training for government personnel, they were able to better demonstrate the impact of vulnerabilities such as 3rd party/ supply chain risks and credentials left in the code.

Invaluable intel regarding leaked credentials and other emerging threats

During initial recon, the unit uncovered a list of leaked credentials sourced from malware logs, and dark commerce sites.

"We were surprised by the fidelity level of the intelligence Argos provided." Says the unit's Guidance Lead, "We have a very strict password policy and you see that the leaked passwords are complicated - this was the real thing. On other systems we often encounter an endless loop of old leaks, but on Argos the intel is up-to-date, accurate and reliable".

"Argos provided us with high fidelity intelligence regarding leaked credentials with zero to near-zero false positives."

A powerful product and partnership

"Argos let me connect with Cyberint analysts right from the alert screen." Says the unit's Senior Analyst, who is in charge of gathering the intelligence, "We're using Cyberint's raw intel, which is pretty clean to begin with - and quick filtering allows us to get to the cleanest intelligence picture regarding critical assets fast."

"Cyberint's analysts and customer success team are always helpful and taught me how to set up effective data filtering to remove false-positives," she continues. "This was especially important during the pandemic, with a lot of noise in the open web."

"We're still training our team and trying to figure out which KPIs we should use to measure the impact," says the Senior Analyst. "Undoubtedly, Cyberint provides our unit with a top layer of essential value."

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