

# CASE STUDY

## ALIAS // CYBERSECURITY CONSULTANCY

**CHALLENGE:** GATHERING ADVERSARIAL INTELLIGENCE FROM DEEP AND DARK WEB DATA SOURCES TO ENHANCE ITS SECURITY ASSESSMENT SERVICE.

**SOLUTION:** DARKIQ



## USING DARK WEB INTELLIGENCE TO ENHANCE SECURITY ASSESSMENTS

Cybersecurity consultancy Alias uses Searchlight Security's DarkIQ solution for its security assessment service, exporting dark web intelligence from the platform to create an informed attacker profile for each individual client, based on the real threats their business faces from the cybercriminal underworld.

Alias provides premier cybersecurity services to its customers including penetration testing, compliance assessments, and incident response, in its mission to protect them from cyberthreats so they can focus on their business. The consultancy was looking for a dark web monitoring solution that could enhance its security assessment service with adversarial intelligence that is specific to each client.

Andrew Noland, Chief Operating Officer of Alias explained: "Seeing a client's weaknesses from an adversary's perspective is the best way to help protect an organization. There are many sources of information that attackers use to do their due diligence and undertake reconnaissance against an organization. Trying to search all of these sources manually is a huge task for our forensic examiners and pentesters so we were looking for a solution that removed this inefficiency. We wanted the ability to identify external threats across the full scope of the clear, deep, and dark web sites and present it back to our clients in a meaningful way."



FOR A SECURITY ASSESSMENT IT IS VITAL TO UNDERSTAND WHAT AN ATTACKER CAN LEARN ABOUT EACH CLIENT. SEARCHLIGHT AUTOMATICALLY GATHERS THAT INTELLIGENCE, HELPING OUR CUSTOMERS TO ASSESS THREATS FROM AN ATTACKER'S PERSPECTIVE.

**ANDREW NOLAND**  
CHIEF OPERATING OFFICER, ALIAS

# CREATING AN ATTACKER PROFILE USING DARKIQ

Alias chose DarkIQ for its ability to continuously monitor across the dark web and identify external threats facing organizations, information which it uses to develop attacker profile reports for each of its clients.

The consultancy is now able to set up a unique account for each client at the outset of its security assessment, input the attributes specific to the organization, and monitor the dark web for indicators of external threat - without having to install anything on the customer's environment. This means that Alias can identify information on its clients in the wild that could be used by criminals to orchestrate a cyberattack - such as leaked credentials, company IP addresses, open or unpatched vulnerabilities, and dark web traffic coming to or from the client's network.

"We chose Searchlight because of the quality of its dark web data sources, which offers a unique view into dark web threats facing our customers," said Noland. "Our pentesters can now efficiently search across a range of marketplaces, forums, and sites, and establish ongoing monitoring for vulnerabilities that are specific to the client - automating a lot of the legwork."

DarkIQ's interface is designed to make it easy for cybersecurity consultancies such as Alias to manage its entire customer base through one multi-tenant environment, without having to toggle between profiles. Insights can be shared with customers through fully automated reporting, which can be customized to include more or less detail, annotations from Alias' pentesters, and fit with the consultancy's branding.

“

WE CHOSE SEARCHLIGHT BECAUSE OF THE QUALITY OF ITS DARK WEB DATA SOURCES, WHICH OFFERS A UNIQUE VIEW INTO DARK WEB THREATS FACING OUR CUSTOMERS.

## NEW COMMERCIAL OPPORTUNITIES FOR DARK WEB INTELLIGENCE

As DarkIQ proves itself to be a valuable enhancement to its current consultancy services, Alias is looking ahead to further commercial opportunities that could involve reselling the product to its larger customers. It believes that mature security teams who have seen the pre-attack insights that can be derived from DarkIQ will want direct access to undertake proactive dark web investigation themselves, as a means to detect new threats or identify data leaks.

"Searchlight is a company that we believe we can grow our services in partnership with," confirmed Noland. "It is a truly collaborative relationship, which we hope to expand through further use of the product with our clients."