SUCCESS STORY

Black Hills Information Security Scales Pentesting Operations With Multi-Tenant Cyber Threat Intelligence

Black Hills Information Security (BHIS) is a Managed Security Services Provider (MSSP) that supports organizations of all shapes and sizes from small community banks to Fortune 100 companies with strengthening their information security infrastructure.

Challenge: Labor-Intensive Homegrown Tool Not Built for Scale

BHIS had built an internal system to collect stealer logs and dark web data, indexing it into an Elasticsearch database. While functional, this homegrown solution created significant operational challenges:

- **Manual processes required constant attention:** The tool demanded continuous oversight. Balancing this maintenance burden with normal job duties became increasingly unsustainable.
- **No path to client access:** As a "garage built" solution using Elasticsearch and Kibana, the tool lacked multi-tenancy capabilities and the authentication and data isolation components necessary to provide clients with direct access to their data.
- **Alternative solutions didn't fit the use case:** The MSSP evaluated other vendors but couldn't justify the spend against the value they returned, and the capabilities were misaligned with what the team needed. These solutions seemed oriented toward OSINT investigations rather than the organization's focus on organizational credentials and infostealer data.

The Customer

Leading penetration testing and cybersecurity training organization

Specializes in offensive security services and continuous penetration testing

Serves organizations across multiple industries including financial services

Any pentest shop not using a solution like Flare to incorporate external threats is doing their clients a disservice. Leaked credentials, especially through stealer logs, are the number one way attackers gain access to organizations.

– Corey Ham,
Director of Continous Pentesting,
Black Hills Information Security

For a pentesting firm where valid credentials represent the primary attack vector their clients face, having reliable, scalable access to dark web intelligence wasn't optional, but was essential to their service delivery.

Implementation: Seamless Transition to Multi-Tenant Platform with White-Label Capabilities

BHIS discovered Flare when fewer vendors were talking about stealer logs. After signing up for a free trial, they found Flare to be a greatly enhanced version of their existing tool. Flare delivered the searchability they demand, but with greater depth and flexibility including the abilities to search specific fields and execute detailed queries.

The "Killer Feature:" White-Label Multi-Tenancy

The ability to create tenants for customers and white-label Flare access as part of their continuous penetration testing subscriptions proved transformative. This became a key element of their service offering. During the trial period, BHIS conducted A/B testing with representative customers, comparing the internal tool against Flare. The results showed Flare's data to be better, with superior search capabilities and manual query options. Unexpected value-adds sealed the deal:

- **GitHub enumeration and enrichment:** Searching for secrets and users across repositories, which was a capability the internal tool never had
- **Credentials browser:** Perfect for password guessing campaigns during penetration tests
- **Optical character recognition (OCR) on dark web chats:** OCR makes previously unsearchable data fully accessible, particularly valuable for financial services clients dealing with check fraud
- **Improved data collection:** Wider range of sources and faster ingest pipeline, with events typically received and triaged by operators within 24 hours

> **Flare made it possible to create an operational center around dark web data for continuous pentesting. We established a triage pipeline that significantly reduced our personal responsibilities in system maintenance while improving reliability.**
>
> – Corey Ham, Director of Continous Pentesting, Black Hills Information Security

Benefit: Scaling and Acting on Dark Web Intelligence

After onboarding with Flare, the MSSP immediately established an operational center around Flare for their continuous penetration testing division. This enabled:

- **Operational efficiency through triage pipeline:** The team created a structured triage pipeline using Jira so team members could investigate alerts, triage threats, and push relevant findings to customers. This dramatically reduced the operational burden on individual team members while improving reliability.
- **Customized alerting capabilities:** Flare's ability to filter by severity, event types, and dates, combined with multiple alerting types, represented a significant upgrade in prioritized alerting from their homegrown system. This ensures that BHIS can receive and investigate events in under 24 hours, which is crucial for reacting to and mitigating infostealers.
- **Infrastructure burden eliminated:** Moving to Flare removed the responsibility of maintaining internal infrastructure and searchability components. The team could focus entirely on analysis and client service rather than system maintenance.

BHIS now uses Flare to test credentials for companies every week.

The real-world impact includes:

- **Daily credential validation:** The team checks newly disclosed credentials daily, regularly finding valid credentials before attackers can exploit them.
- **Active account compromise prevention:** Triaging stealer log events surfaces active session cookies and stops account takeovers before attackers can act.
- **Financial services protection:** Medium-sized banks without their own dark web monitoring solutions benefit from catching check fraud and consumer account sales on the dark web.
- **Direct client investigation:** Customers with direct access to their Flare tenant can investigate alerts independently, reducing response times and empowering client security teams.
- **Industry-wide risk reduction:** By incorporating infostealers and dark web data into their pentesting methodology, the MSSP helps reduce the industry-wide risk associated with valid credentials being the primary breach vector.

Forward Look: Scaling and Futureproofing their Services

BHIS's journey from a labor-intensive homegrown tool to a scalable, multi-tenant dark web intelligence operation illustrates what's possible when the right data meets the right platform. By replacing manual infrastructure maintenance with Flare's searchability, white-label tenancy, and triage-ready alerting, the team freed up time to focus on what they do best: finding and validating real attack paths for their clients.

Flare empowers BHIS on delivering continuous penetration testing: powering daily credential checks across dozens of organizations, catching active account compromises before threat actors can exploit them, and giving clients direct visibility into their own threat exposure. Having comprehensive, scalable access to stealer log and dark web intelligence isn't just a nice-to-have, it's a key part of the service.