SUCCESS STORY

MSSP Secure Coders Upgrades Threat Exposure Monitoring for Multinational Pharmaceutical Company

The Customer

Secure Coders: boutique security consulting firm, works with early stage startups all the way to Fortune 100 companies

Secure Coders' client: pharmaceutical company with distributed teams

> "Even in the initial proof of concept for our pharmaceutical customer, we increased visibility of scale with several escalated alerts and gained knowledge of systems that showed significant risk."
>
> -Secure Coders

Challenge: Multinational Pharmaceutical Company Needs Holistic View of their Exposure

A multinational pharmaceutical company had an information security program that lacked a comprehensive view of their exposure on the clear & dark web. Their goal was to get a better understanding of how an exposure monitoring solution can provide value and security to enforce the organization's control objectives, as well as how clear & dark web monitoring can provide ongoing visibility into the organizations' data security objectives. They reached out to Secure Coders who partnered with Flare for the engagement.

To help manage their goal and better understand the unique needs of the organization, the Secure Coders team utilized Flare to conduct an exposure monitoring proof of value. This proof of value included a feature demonstration and a high level assessment of the organization's external exposure. When the Secure Coders team uncovered results indicative of risk using the Flare platform, they used that data to improve monitoring for similar types of risk on a continuous basis.

With interesting results in hand, the Secure Coders team put on their red-teaming hats to analyze findings as an adversary would to illustrate potential impact and recommendations to resolve or mitigate the risk.

Implementation: MSSP Offers Comprehensive Proof of Value to Client

The Secure Coders team conducted the following efforts.

Phase	Duration	Description

Develop Requirements	**1 week**	• Meet with the organizations leadership to develop business requirements through the following:
		  ◦ Document Process
		  ◦ Document Focus Area
		  ◦ Document Threat Escalation Process

Exposure Monitoring and Reporting	**4 weeks**	• Monitor and report on threats identified based on the documented requirements through the following:
		  ◦ Regular Reporting of Threats
		  ◦ Weekly Review and Touchpoints
		• Continuously communicate with the organization's leadership to refine requirements as inter-organizational processes mature.

Engagement Review and Future Planning	**1 week**	• Meet again with the organizations leadership to reassess requirements for continued exposure monitoring through the following:
		  ◦ Engagement Overview / Summary
		  ◦ Continued Service Scoping and Proposal

The table below outlines the process employed by Secure Coders to identify, enrich, prioritize, and remediate threats.

Exposure Monitoring Process	Description
Identification	Discover risks from a wide coverage of sources where employees, or adversaries may leak data, or compromise the integrity of the organization's brand by counterfeiting, or reselling products without proper consent.
Enrichment	Enable automated data regrouping and enrichment using open-source intelligence gathering.
Prioritization	Prioritization using sophisticated tools and manual review of risk for each issue identified as determined by the organization's management specializes in employee error detection. Issues were reported to the organization based on criticality.
Remediation	Discuss process for executing takedown and notifying/training employees.

Using its expertise and the Flare platform, the Secure Coders team made the following capabilities available.

Criminal underground monitoring

- **Access Brokers** - Provide actionable intelligence that saves time spent to detect and remediate attacks or compromised systems for sale on dark web marketplaces.
- **Forum Chatter** - Classify and report on conversations occurring on dark web communication channels relating to brand, product, and operations.

Intellectual property monitoring

- **Publicly Posted Source Code** - Review publicly available source code posted by both internal and external entities to the organization. Source code is analyzed and reported on by experienced software developers.
- **Public Dumps** - Review content posted on channels such as Pastebin that pertains to the organization's brand.
- **Public Forum Disclosures** - Monitor public forums for discussions which disclose sensitive internal information.

Monitor external attack surface

- **Monitor Github for Source Code and Secrets leakage** - Monitor online code repositories for accidentally leaked information. Run custom regexes and queries that cross public code repositories such as GitHub, BitBucket, and GitLabGit-environments.
- **Detect Technical Data Leakage** - Detect mistakes and secrets being committed about the organization's environment and send alerts to the security team on accidental commits.
- **Identify Misconfigured Servers** - Enable real time notification of S3 storage, Shodan, and other cloud data that could put the organization at risk.
- **Monitor Anonymous Sharing websites** - Monitor password dumps, sensitive technical data, and PII that is posted on Pastebin and other anonymous sharing sites (bin sites).

Preventing account takeover

- **Real-time Credential Monitoring** - Collection of leaked credentials from the dark, deep and clear web, ensuring they can't be abused the minute they are discovered
- **Automated Workforce Account Monitoring** - Integrated credential dump feeds with the organization's existing processes.

Brand protection

- **Drug Marketplace Monitoring** - Continuously monitor product and service postings on dark web marketplaces relating to product sales and counterfeiting.
- **Dump Monitoring** - Monitor dumps advertised pertaining to the organization's business.

Detecting phishing attacks

- **Subdomain Monitoring** - Identify phishing domain names and SSL certificates and detect the registration of new domain names similar to the organization's domains.

Preventing financial fraud

- **Workforce Protection** - Search directory of financial fraud victims, based on leaks on the dark, deep and clear web, as well as on identities for sale on illicit markets. Enable the organization to check if their workforce have been victims of fraud, while ensuring information privacy protection.

Benefit: Escalated Alerts from Exposure Monitoring Provide Valuable Knowledge on Significant Risk

Through the proof of value, we were able to demonstrate the benefits and value of implementing an exposure monitoring solution. Secure Coders using Flare successfully increased visibility of the organization's external exposure on the clear & dark web. The following were delivered through the course of the proof of value:

- 1,590 Flare identifiers were created
- Monitor External Attack Surface report with 1 escalated alert
- Intellectual Property report with 9 escalated alerts
- Leaked Credential report with 1 escalated alert
- Monitor External Attack Surface report with 6 escalated alerts
- Preventing Financial Fraud report with 5 escalated alerts

Several of the escalated alerts resulted in the organization gaining knowledge of a system that presented significant risk. The organization requested a follow-on engagement for an advanced persistent threat (APT) style pentest targeting the system, which was performed by Secure Coders utilizing their team of experts, heavily leveraging the Flare system.