SECDO | CASE STUDY

PAYONEER MULTIPLIED THE EFFICIENCY AND EFFECTIVENESS OF ALERT INVESTIGATION WITH SECDO

BACKGROUND

Payoneer empowers customers to grow their businesses by enabling them to pay and get paid as easily globally as they do locally. Payoneer enables millions of businesses and professionals from more than 200 countries and territories to reach new audiences by facilitating seamless, cross-border payments.

A combination of greater trust and ease of use means customers are increasingly opting to do their business digitally. Online transactions are growing by 10% per annum, and avoiding cyberattacks is the number one priority.

Payoneer is all about trust. All parties to a transaction must be able to rely on the veracity of the information. Payoneer's customers place a great deal of trust in the hands of the company and they must have faith in Payoneer's ability to hold their confidential financial information securely.

Like all financial companies, Payoneer is aware of the threats of cyberattacks and is on the perpetual lookout for new technologies to ensure the safety of their platform.

Payoneer

FOUNDED
2005

EMPLOYEES
1000

INDUSTRY
Financial Services

HEADQUARTERS
New York, USA

OPERATIONS
200 countries

RESULT WITH SECDO
Effective alert investigation

CHALLENGES

Payoneer maintains thousands of endpoints and servers in numerous countries, all of which are potential targets for attack. Payoneer's team of security analysts manually investigate alerts generated by the different detection and prevention systems deployed on the company's network and endpoints. Alert investigations are laborious and time-consuming, as it necessitates the analysts to collect data from endpoints and servers to try and pinpoint the root cause and determine the impact. But without visibility into historical activity on every endpoint and server, the investigation process at Payoneer is arduous and may be incomplete and inaccurate.

Payoneer's senior security analysts also needed the capability to go on the hunt proactively against threats that show up in intelligence feeds or that are publicized by other organizations.

SOLUTION

After researching existing endpoint-focused solutions, Eliran Radai, Payoneer's Cyber Security Manager, decided to conduct a proof of concept for Secdo's incident response platform.

Secdo's agents continuously collect all endpoint and server activity and store it on a centralized server, on-premise or in the cloud. Secdo's algorithm, the "Causality Analysis Engine" continuously analyses the endpoint events, grouping them into "Causality chains". Secdo then integrates with any SIEM or detection system to ingest alerts and correlate them with the already established causality chains, instantly revealing the full context of each alert, including the forensic timeline, attack chain, root cause and damage assessment. With a clear knowledge of exactly what happened on the endpoints, security teams can then use Secdo's response and remediation tools to immediately contain the infected process and completely remediate the threat.

> *Using Secdo, we were able to get to complete the investigation, very soon after an alert came in".*
>
> *Eliran Radai,*
> *Cyber Security Manager*

RESULTS

After only a few hours of setup, the Secdo agents were collecting all events, behaviors, and actions on Payoneer's endpoints without affecting the end users at all. All endpoint data was sent to the Secdo cloud and stored.

Once the integration with the SIEM and 3rd-party detection systems was established, alerts began to flow automatically to the Secdo system which immediately correlated each alert with its specific causality chain, establishing a complete forensic timeline.

Instantly, Secdo revealed the entire history of each alert, from its root cause. Based on Secdo's automatic investigation, Payoneer's analyst were able to speed the process of validating each alert.

"This was exactly the kind of information we would obtain after a lengthy investigation," stated Radai. "Using Secdo, we were able to complete the investigation, very soon after an alert came in."

As root cause of incidents is revealed, Paynoeer's team was also able to spot holes in their defenses and address it, reducing the risks of similar attacks in the future.

Payoneer's security analysts also used Secdo's Query Builder, so they were immediately able to hunt for new threats on their own. With Secdo, one queries the historical database, not the endpoints themselves, so the data is always available and the searches are fast. With Secdo, even an advanced threat that executes, then deletes all traces from the endpoint, its sub-second activity is captured in the database and analysts can easily find it. Nothing escapes Secdo's visibility into endpoints.

> *After the successful POC, we implemented Secdo across all of our endpoints and our security team is now working on a daily basis with Secdo, investigating alerts and conducting threat hunting. Using Secdo, our security staff is more efficient and effective and our business is even more secure".*
>
> *Eliran Radai,*
> *Cyber Security Manager*