INTEZER

Case Study — legato security

Legato Security scaled up SOC analysis with automation to deeply investigate alerts

About Legato Security

Legato Security provides their clients with comprehensive cybersecurity expertise, designed to provide 24/7 monitoring and immediate response to threats.

Learn more at www.LegatoSecurity.com/

Top Challenges

- High volume of alerts from different clients, with too many files and URLs to manually analyze
- Need to maintain privacy for potentially sensitive data that could get uploaded for analysis

Solution

- Automation with Intezer extracts and analyzes artifacts from any alert, giving them fast results about every suspicious file and URL
- Privacy for every sample analyzed by Intezer, whether the sample was uploaded manually for on-demand analysis or collected automatically

Benefits with Intezer

- Definitive verdicts and actionable intelligence
- Time savings from automation, fast analysis, and ease of use
- Private sandboxing to prevent sharing of their client data

The Challenge:

Too many alerts to deeply investigate all the related artifacts

Jesse Stoltz, the SOC manager for Legato Security, leads a team of 20 cybersecurity professionals who provide 24/7 monitoring and alerting services for a multitude of clients.

With a growing company and client base for Legato Security, Jesse and his SOC team needed to find an automated solution for malware analysis.

Manual analysis couldn't keep up with all the suspicious files and URLs produced from their alerts. Some tools that could have helped them with analysis didn't give them the privacy they needed for their samples, to avoid sharing private client data.

While researching different options, they found Intezer and started trying out the free version's powerful features for file and URL analysis.

Jesse Stoltz
SOC Manager

> There is a large volume of alerts produced every day and manually performing analysis on all of these files is not scalable.
>
> Intezer has given us the ability to provide in-depth reporting in a timely manner. Moreover, having a private instance for us to upload potentially sensitive data was a 'must have'.

The Solution:

Automating analysis of suspicious files and URLs from alerts

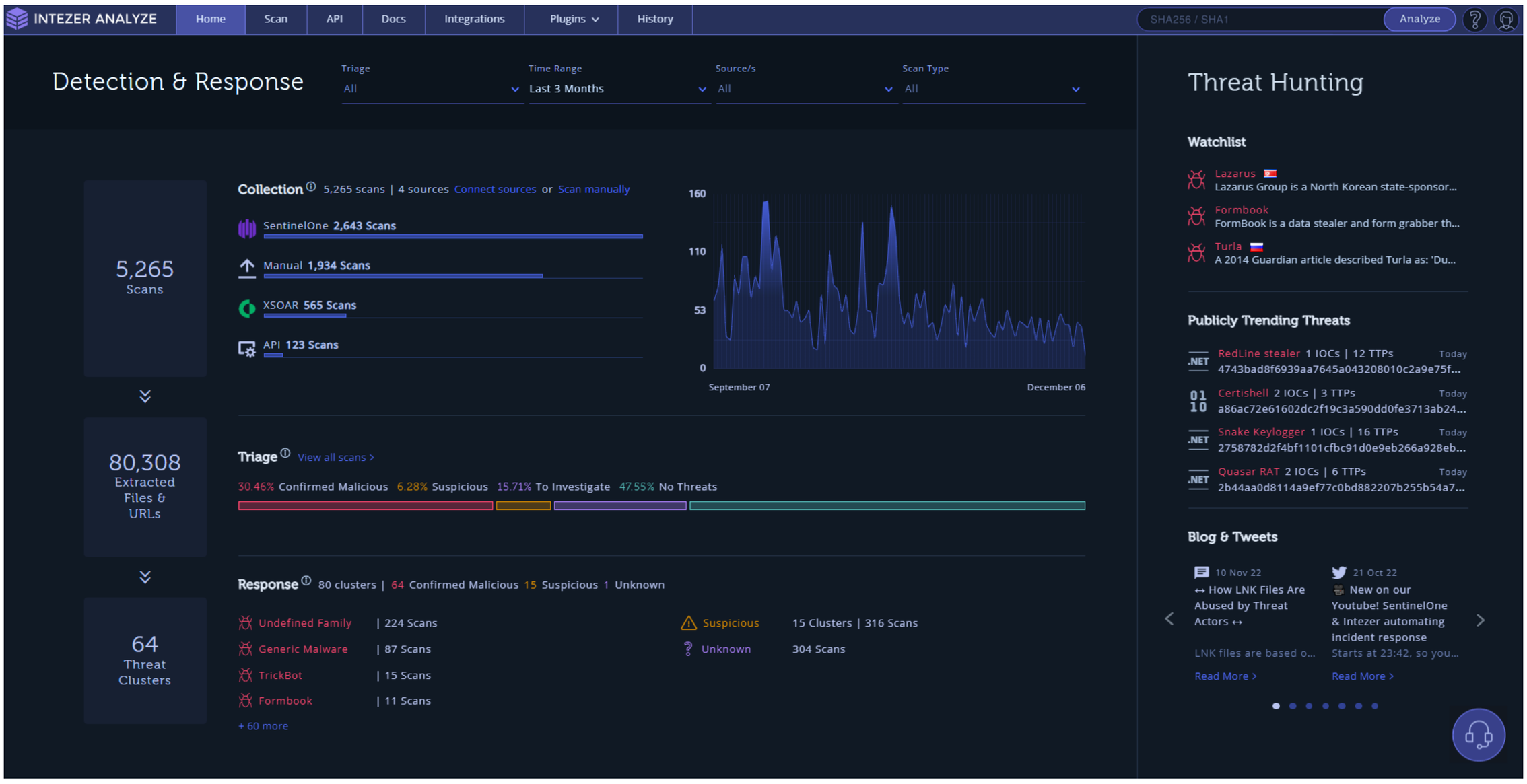
When Jesse's SOC team began using Intezer, they realized they could get the sandboxing features they were initially looking for as well as a suite of more powerful tools for triage, investigations, and hunting.

The implementation process for his team was incredibly smooth according to Jesse, with responsive and helpful support from Intezer along the way. His team found Intezer fit right into their processes as a "plug and play" solution to connect with CrowdStrike, without needing much maintenance or overhead from the team.

Now, the SOC analysts on Jesse's team are using Intezer constantly – "all day, every day," he says. In addition, they're able to leverage the IOCs (indicators of compromise) extracted by Intezer to enable their detection engineering and develop higher-fidelity alerts.

Over one 3 month period, Intezer performed 932 scans for Legato Security's team. Those scans included artifacts collected automatically by Intezer, as well as any files the team uploaded for on-demand analysis. From all those scans, **Intezer extracted and analyzed 10,228 files and URLs,** ultimately classifying the detected malicious code into 25 distinct threat clusters.

In one instance, the team got a potential ransomware detection which Intezer confirmed as likely ransomware activity. Based on the additional information from Intezer, the SOC team was able to respond to the event more quickly. While responding to the incident, they also used Intezer's endpoint scanning tool to gather and report on additional forensic evidence.



An example of Intezer's dashboard, which shows the sources for alerts, triage results from Intezer's analysis, and threat clusters for confirmed threats.

Expanding with Intezer

Since onboarding with Intezer, Jesse and his team have benefited from ongoing improvements and new features that allow them to do much more than what traditional malware analysis solutions provide. They're exploring even more use cases with Intezer's API.

Jesse is looking forward to leveraging Intezer's Detect & Hunt features more over time. Detect & Hunt gives them out-of-the-box detection content so they can quickly generate effective hunting rules, with high accuracy and low false-positive rate. It also enables them to create detections targeting threat actors and malware families – something that's a game changer. With Intezer, he's expecting they'll be able to start automatically hunting for threats in their environments.