CYREBRO Alert Lifecycle

1

Collectors are data gateways that gather data (logs sources from cloud, on-prem, endpoints, machines, etc) from clients' environments and send it to CYREBRO.

2

The data is then parsed on the SIEM, a dedicated cloud environment. Meaning the data is broken down into a readable format, ie the source IP and destination IP.

3

The data then enters the data lake where it is mapped and normalized. This is to better understand what the data is telling us based on parsing (i.e. failed log-in attempts). Here, CYREBRO begins looking at "events of interest" from all of the data received.

4

The "rule engine." AI detections kick inby continuing to look at the parsed data to identify "events of interest". This uses a combination of AI technology, rules, and correlations. Events are then correlated to create corresponding offenses.

5

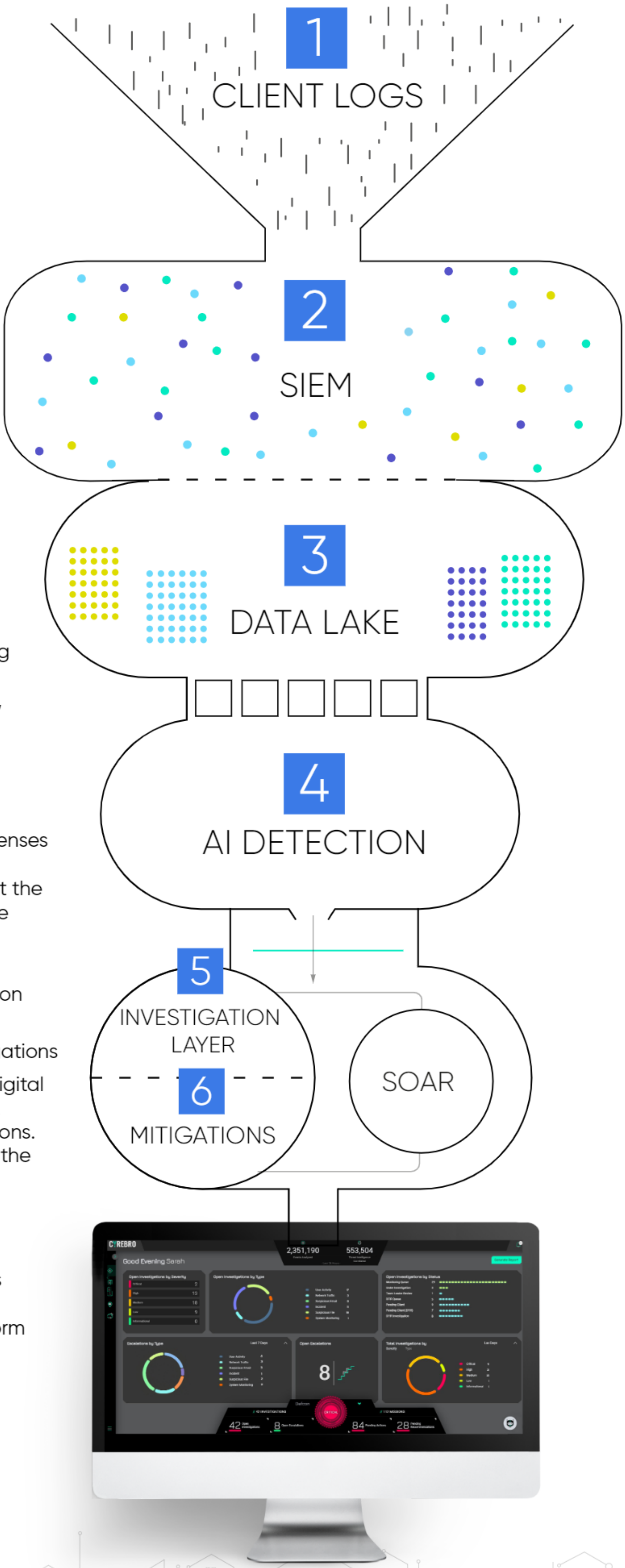
Next, the SOAR correlates and aggregates the offenses to determine the attack story, and creates an investigation in the CYREBRO Platform. Throughout the detection, investigation, and mitigation stages, the SOAR system is responsible for:

- Creating an attack story
- Automatically enriching the data (i.e., geolocation resolving for IP addresses, known bad IPs, etc.)
- Automatically investigating and closing investigations

The strategic monitoring, incident response, and digital forensics teams work in conjunction with the SOAR technology to review, close, or escalate investigations. An alert is generated in the CYREBRO Platform for the end-user (client) with detailed information

6

After investigating, the monitoring and DFIR teams will deliver mitigation steps to the client directly in the CYREBRO Platform. These steps come in the form of recommended remediation steps and actions required from the client to mitigate the incident.



www.cyrebro.io
info@cyrebro.io

Headquarters:
52 Menachem Begin Street,
Tel Aviv, Israel

US Office: 38 High Avenue
4th Floor. Nyack, NY, 10960