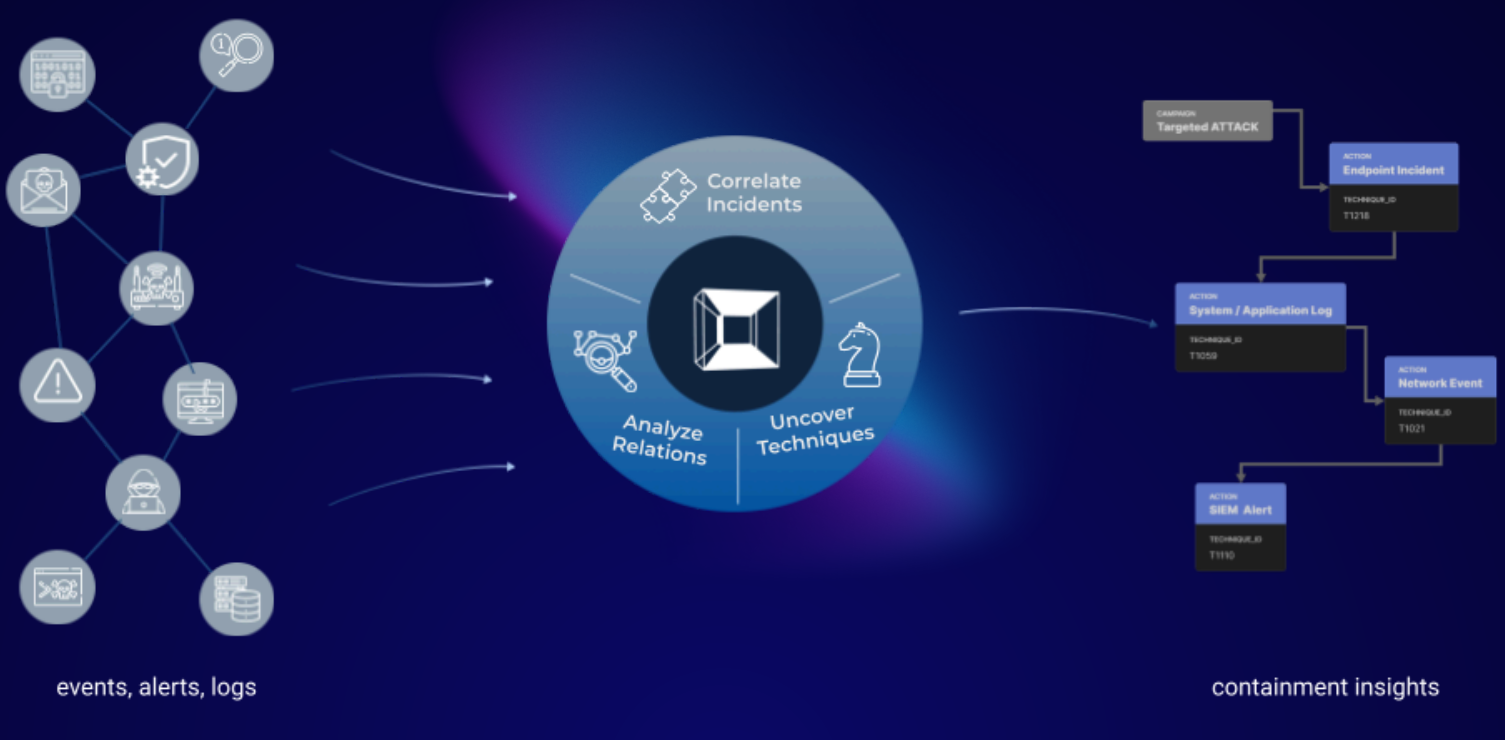
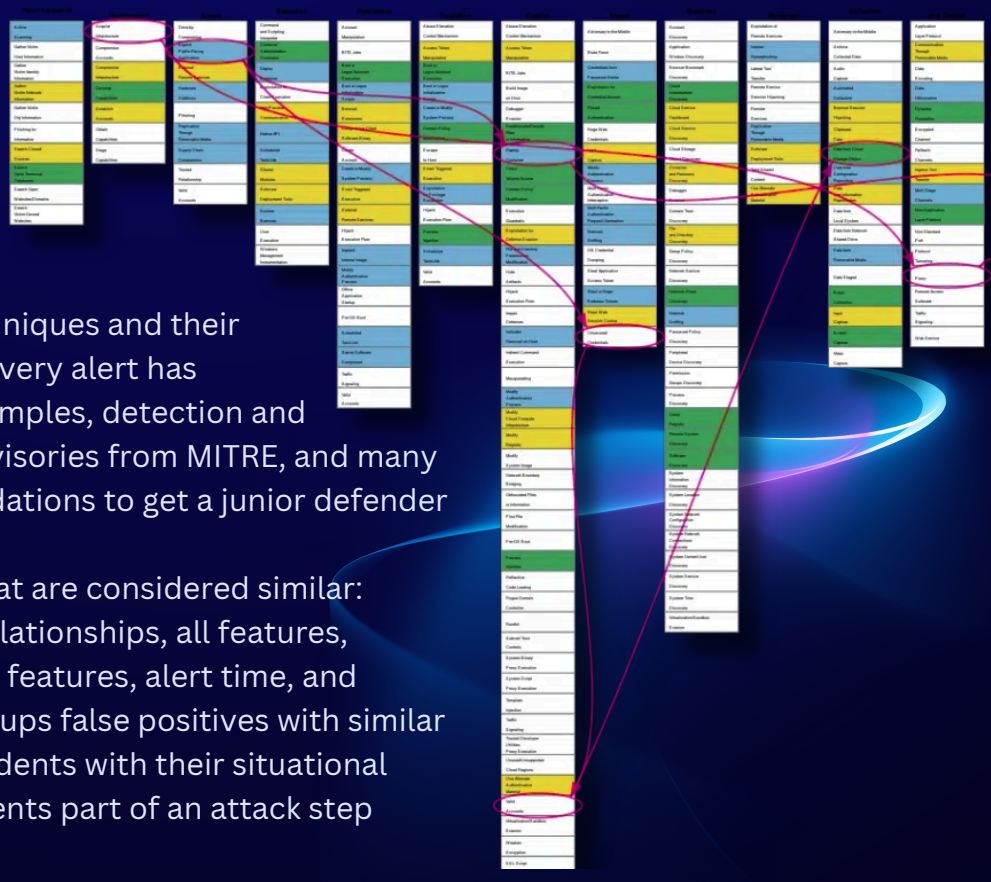
Contextualizing Incidents

Cypienta is an air-gapped rule-less solution to continuously contextualize and correlate Alerts, Events, and logs. It augments and attaches directly to your technology stack (Any SIEM, SOAR, XDR, Case Management, etc.) to enhance your SOC's efficacy and efficiency by presenting relevant data points to each incident.



Connect the dots
See the entire Attack Flow



Given alerts of any format, or type, Cypienta models output the following in real-time without rules or training:

- Relevant MITRE ATTACK techniques and their probabilities for each alert: Every alert has explanations, procedural examples, detection and mitigation guidelines and advisories from MITRE, and many more details and recommendations to get a junior defender to act as a senior defender.
- Clusters of relevant alerts that are considered similar: Based on involved entities relationships, all features, custom attributes, identities' features, alert time, and relevant techniques. This groups false positives with similar root causes, groups lone incidents with their situational awareness, and groups incidents part of an attack step together with their context.
- A sequence of alert clusters that is causal, representing a MITRE attack flow or a cyber kill-chain: This exposes coordinated and targeted multi-step attacks (common in APT, Cyber Warfare, and Cyber Criminal campaigns), allowing defenders to see the big picture even when undetectable 0-days or blind spots affect the observational coverage of certain key steps, the other traces left behind are sequenced to reveal the attack path.