empow

You have it in you.

i-SIEM

Donnelley Financial Solutions

> empow is unique in the security arena...it makes all the tools in our arsenal work optimally and in a synchronized way so that our level of security is effectively improved.

> With empow, I have the confidence of knowing that my security organization is responding in the right way, every single time.

Dannie Combs, SVP and
Chief Information Security Officer

MIT Media Lab

> As a university, we need to share things, to be open, but still protect our users privacy - this makes us a big juicy target for cyber attackers.

> empow allowed us to optimize our security coverage, while ensuring privacy and extending visibility of what is happening in our network"

Michail Bletsas, Director of Network
and Computing Systems

Recognition & Awards

SC 2019 awards Winner

"... Replacing the security Tower of Babel of existing point solutions..."

Forbes

Gartner Cool Vendor 2017

"empow's models generate a small set of strategic rules, as opposed to the hundreds or thousands that are present in most Security Information and Event Management (SIEM) systems.

SC MEDIA

"...empow has earned its place among the top solution providers in its category."

"Breaking through the cybersecurity bubble"

NETWORKWORLD FROM IDG

9 Patents Granted,
6 Patents Pending

The Challenge

Organizations today are challenged in selecting the right technology for their cyber security needs. Experience – their own or others' – has taught them that SIEMs are complex and require a long time to implement, tune, and maintain. Moreover, once implemented they require a large security team to write correlation rules, sift through the many false positives, and manually research events in an ever increasing threat landscape. All this makes SIEM projects expensive, with the total operational cost and management far beyond just the cost of the software. These reasons lead many organizations with small security teams to delay the implementation of a SIEM or turn to alternative solutions.

i-SIEM

An intent-based system, i-SIEM is based on Artificial Intelligence (AI) and Natural Language Processing (NLP) algorithms, reinforced with User Entity Behavior Algorithms (UEBA) and Network Traffic Analysis (NTA) engines, that together enable an automated classification and prioritization process. This automation enables i-SIEM to eliminate the manual process of writing correlation rules. i-SIEM analyzes, prioritizes and delivers a very small number of truly high-risk entities to security analysts (preventing alert fatigue and unnecessary false positives generated by other SIEMs). This means organizations can implement a comprehensive cyber security strategy, effectively managed by less than one security analyst.

Benefits

While many other SIEM systems are expensive and take a long time to tune, i-SIEM has many benefits.
No longer do you have to settle for limited security use cases or attack patterns, volumes of false positives, or complex correlation rule writing. Gone is the massive expertise needed to run a SIEM. Gone is the expense.

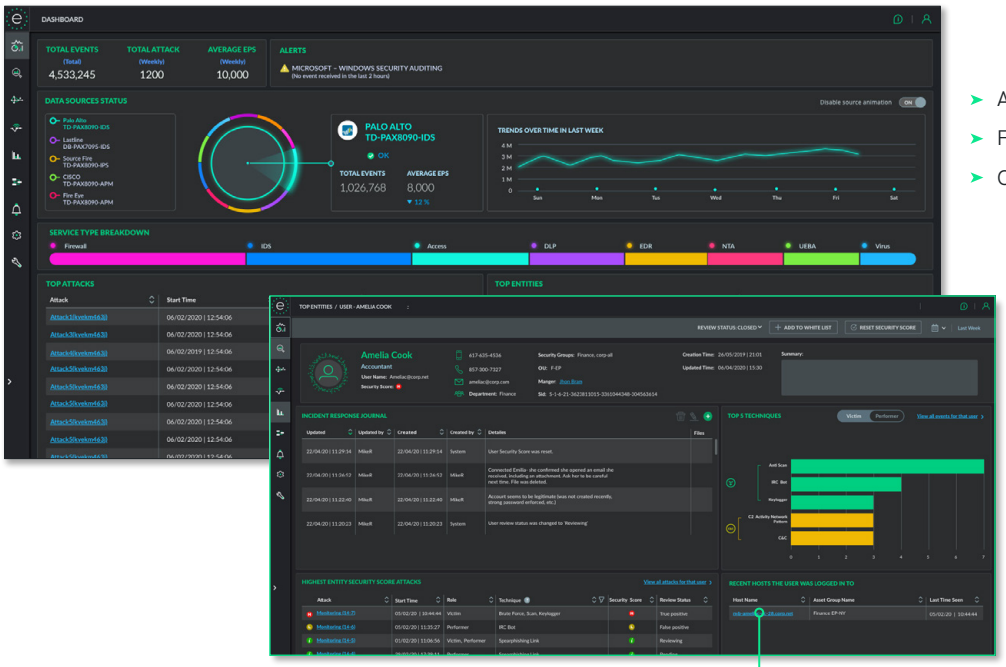
- Wide coverage – automatically correlates security logs to identify advanced threats (no manually generated rules required)
- Proactive – powerful AI enables constant identification of new attack patterns
- Automated investigation & response processes
- Reduces false positive rates by an average of at least 90%
- Seamless data digestion based on empow's data classification technology
- Best in class data lake with full Elastic log analytics premium features and largest community enriching it
- High ROI thanks to seamless integration, virtually no maintenance costs

User Experience

i-SIEM automates the analyst's workflow. Instead of analysts working their way through volumes of false positives, i-SIEM works in the background to classify, enrich, and prioritize all security events. The security analyst gets presented with only the true, high risk attacks, reducing alert fatigue and making the process more efficient. Analysts can now act with confidence and work more effectively with all the details at their fingertips.

Not only does i-SIEM automate the classification and enrichment process, but it also automates the remediation workflow by opening tickets on ServiceNow or other ticketing systems once an attack is confirmed. Pre-defined integrations coupled with custom alerting means you can connect i-SIEM to third party security operations systems to further streamline your workflow.

Real Time Monitoring of Prioritized Entities

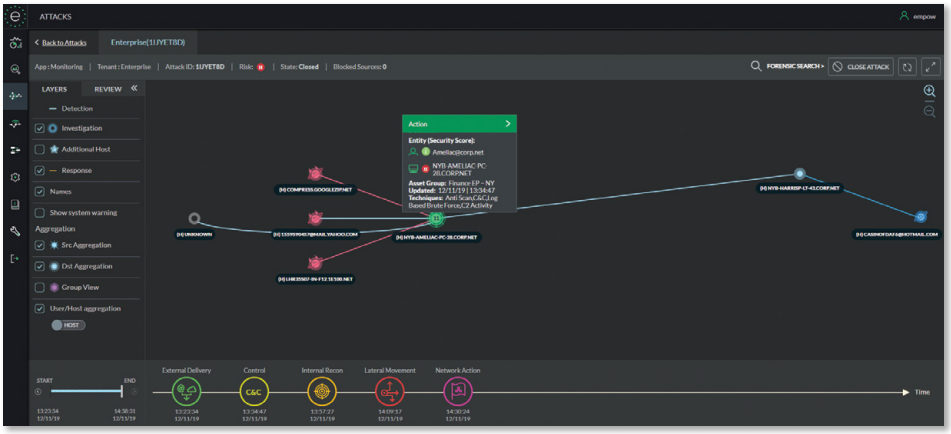


- Auto prioritization
- Focus on highly sensitive entities
- One common language

Entity Card

- Entity's organizational context
- Impact analysis score

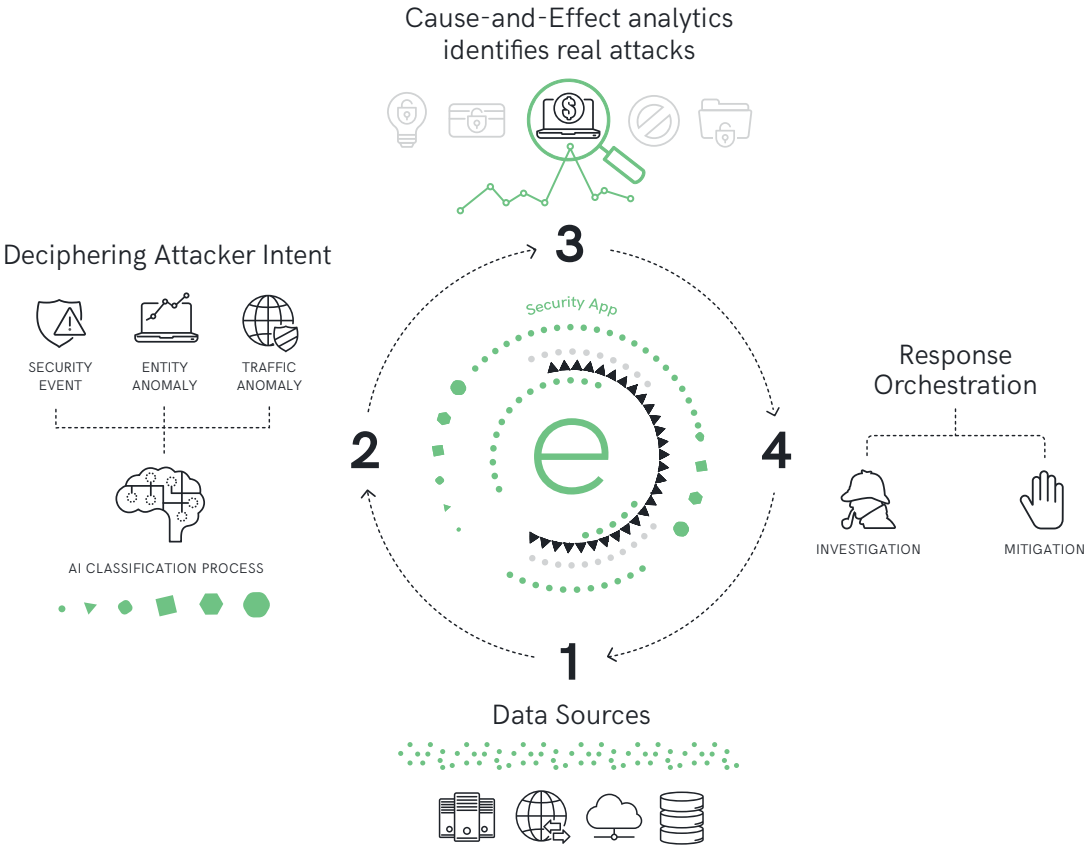
Attack Story



- Visualize time-based attack story
- Quick root-cause analysis
- Advise response types
- Enables forensic search & hunting

How It Works

i-SIEM comes with a built-in library of plugins that feed data into the system from a variety of sources. i-SIEM then classifies, normalizes, and analyzes the data according to customized defense models and the MITRE ATT&CKTM framework, using patented technology only available in i-SIEM.



1/ Data Sources

The integrated i-SIEM empowered by Elastic collects all types of IT data including security logs, security intelligence feeds, OS logs, servers and application logs, network flow data and more, by using a range of available data source plugins.

2/ Deciphering Attacker Intent

empow's AI and unique NLP (Natural Language Processing) algorithms and Adaptive Expert Engines classify attacker anomaly behavior and intent into the MITRE ATT&CK common language. Three main types of malicious intent classifications are done: User entity anomaly classification, network traffic anomaly classification and security events classification.This process runs continuously and automatically, with virtually no human involvement, and marks the logs and events with intent metadata which is indexed into the Elastic DB. Examples of intent classification include: Internal recon, external delivery types, local and remote privilege escalation, PII data scraping, financial data scraping and ransomware and more MITRE classes.

3/ Cause-and-Effect Intelligence

empow's security analytics engine identifies cause-and-effect relationships between the collection of deciphered intents, grouping them together and prioritizing the real attack stories and compromised entities in the organization.

This engine emulates human security expert processes, identifying the real attacks out of all the noise and deciding, according to the attack intent, which investigation policies are required, and which proactive response policies to employ.

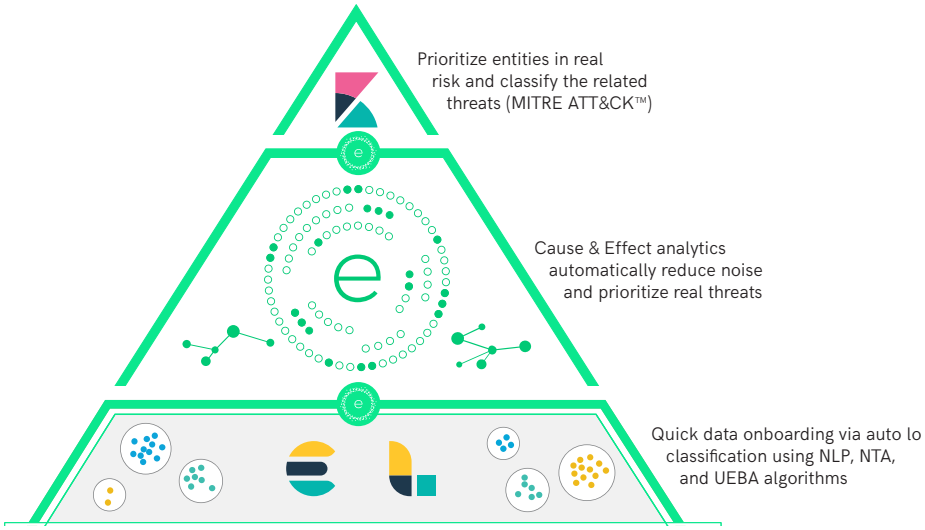
4/ Response Orchestrion

empow's Contextual Orchestration Engine dynamically identifies and selects the best available products and network tools to execute the investigation and response actions. This translates into fast and optimal incident response, while at the same time simplifying security operations and eliminating maintenance overhead.

i-SIEM – built on Elastic

SIEM platforms need to collect large volumes of IT data from installed sensors in the organization, process it and provide rapid access into it. To streamline this process empow has partnered with Elastic, the leader in data search with over 300 million users. empow's patented technology, integrated into the Elastic framework, allows unparalleled database search capabilities, on top of a long-term retention data lake. Customers can take advantage of the full Elastic Platinum Node features (including alerting, monitoring, reporting, machine learning, canvas, Elastic Search SQL, graph algorithms & others) included by empow as part of i-SIEM.

In the figure below, we show how i-SIEM takes advantage of Elastic's Logstash, Beats and Kibana tools to create a more effective SIEM solution. Beginning at the bottom of the pyramid, empow enriches every security event with the attacker intent during data ingestion. After processing, these enriched logs are then stored in Elasticsearch, allowing analysts to conduct much more efficient investigations and forensics operations. i-SIEM then applies cause & effect intelligence, which automatically correlates all classified events and prioritizes the attacks and entities as real risks. At the top of the pyramid, empow utilizes the Kibana framework to clearly deliver visualizations and dashboards of high risk attacks and entities, allowing easy drill-down into the most relevant data. This integrated combination delivers automation, predictive analytics, and long-term retention to enterprises and service providers in a scalable, security-optimized solution. The overall solution provides a top-down analysis experience for identifying attacks, all without manually generated rules.



Defense Models

i-SIEM provides pre-built, customizable, defense models that allow organizations to define what risks and compliance requirements are in focus, enabling i-SIEM to optimally detect attacks with the relevant malicious intents, and orchestrate investigation and response accordingly. i-SIEM enables users to define models by using the MITRE ATT&CK™ language, making classification unified and translatable.

Security Models can be easily downloaded from empow's security use cases library and implemented in minutes. Pre-built models cover both basic and advanced security use cases including: Insider threats, data exfiltration, privilege escalation, identity theft and account take over (ATO), phishing and social attack campaigns, various investigation flows, and more. Each model is capable of detecting and responding to advanced threats, including:

- **Ransomware**
- **Identify Theft & account take over**
- **Intelligence gathering**
- **Phishing & social attack campaigns**
- **(ATO)Insider threat**
- **Data-leak**

UEBA & NTA Engines

i-SIEM comes with out-of-the-box User Entity Behavioral Analytics (UEBA) and Network Traffic Anomaly (NTA) engines (supported by empow's DPI network agents) that learn and profile the normal behavior patterns of users, applications and traffic, and detect anomalies based on deviations from these patterns.

These engines add an important layer to your detection system:

- They spot suspicious and abnormal behaviors that indicate an attacker is already in the environment or a bad insider is active – otherwise missed by signature-based or heuristics tools and static SIEM rules based on thresholds.
- They identify a critical visibility gap, where most organizations only deploy perimeter and host-based tools, leaving their internal networks, cloud and user activity unmonitored.
- They can help triage, confirm and complete attack stories by discovering additional attacker steps along the cyber kill chain.
- Providing these as integrated, out of the box features of i-SIEM enables alerts that are automatically classified by attacker intent, with no correlation rules.

Classification based on Threat Intelligence

i-SIEM integrates threat intelligence real-time feeds from various 3rd party sources, including commercial as well as open ones, in order to enrich the system with information which allows automating logs classification and investigation processes. The TI based classification process allow to:

- Translating all logs into one language of MITRE ATT&CK even when the logs' native description are vague or don't exist
- Classify benign logs, i.e., remove noise and false positive
- Identify and classify bad reputation sites

Data Sources Integrations

A range of plugins for 3rd party networking, servers and security data sources are included in empow's offering, such as intrusion detection systems (IDS), network anti-malware, security reputation services, endpoint protections, firewalls, OS logs, Domain Controllers, Cloud based application, and many others. If needed, new plugins can be developed by empow's eco-system integration team, or by using the community contributed Elastic Logstash plugins.

i-SIEM's ecosystem supports products from dozens of vendors, including:

paloalto NETWORKS · lastline · McAfee · Symantec · cisco · FORCEPOINT

cybereason · TREND MICRO · SOURCEfire · Carbon Black. · Check Point SOFTWARE TECHNOLOGIES LTD · WAZUH

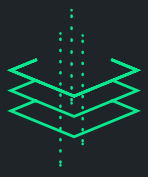
CYLANCE · FIREEYE · SOPHOS · WEBROOT · ANOMALI · f5

JUNIPER NETWORKS · Microsoft · CROWDSTRIKE · eset · SNORT · FORTINET

Benefits -
Shortcut to Mature Security

Early detection of advanced threats, known and unknown - No rules !

Speed of Investigation and response (in seconds rather than days)



Visibility across all your environments

Improved ROI - priced per hosts, not data

Turn What You Have Into What You Need

empow
You have it in you.

Tel: +1-877-647-4361
129 Newbury Street, 2nd Floor
Boston, MA 02116, United States

Tel: +972-3-519-5517
Hayetzira 29, Ramat Gan,
Israel 5252171

www.empow.co
info@empow.co