empow

You have it in you.

# i-SIEM

## empowered by Elastic

**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 EUROPE 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

7 Patents Granted,
9 Patents Pending

# The Barriers to SIEM

Organizations today are weary of entering into a SIEM "project". Experience – their own or others' – has taught them that SIEMs are complex and require a long time to implement. Moreover, once implemented they require a large security team to manage – write correlation rules, sift through many false positives and more. The fact is that humans can't search the cybersecurity data and write security correlation rules that represent attack patterns as fast as machines can generate new attacks. All this also makes SIEM projects expensive, with "cost creep" and management costs far beyond 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 like MSSP providers.

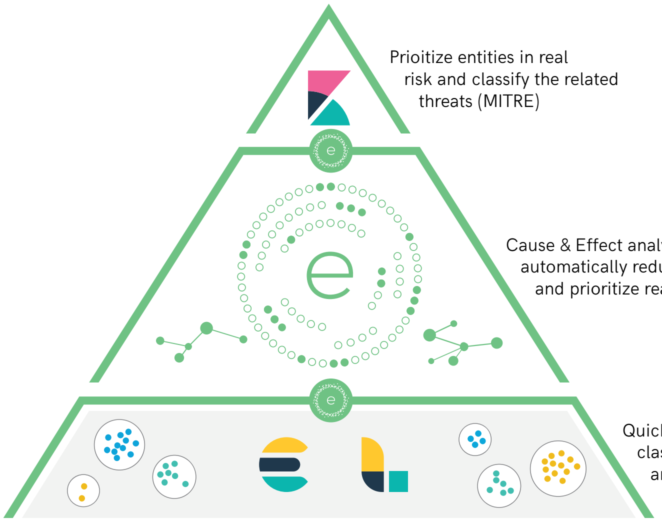
# i-SIEM empowered by Elastic

empow's patented intent-based SIEM (or i-SIEM) technology is based on AI and Natural Language Processing (NLP) algorithms, reinforced with UEBA and NTA engines, that together enable an automated classification and prioritization process. This automation enables i-SIEM to bypass the whole process of writing correlation rules. i-SIEM's process results in a very small number of truly high-risk entities (minus the mountains of false positives generated by other SIEMs), that can be effectively managed by less than one security analyst.

SIEM platforms need to collect all the IT data in the organization and provide very fast access into it. To streamline this process empow joined forces with Elastic, the leader in data search with over 300 million users, in a strategic OEM partnership. empow's unique "rules-free" SIEM technology, integrated within Elastic's database and search capabilities, deliver the most streamlined, effective SIEM in the market. The integrated solution provides medium to large enterprises and service providers a scalable security-optimized "data lake" solution.

empow also provides customers with the full Platinum license Elastic features (including alerting, monitoring, reporting, machine learning, canvas, Elastic Search SQL, graph algorithms & others) as well as Elastic vendor support.

In the figure below, we show how empow's i-SIEM integrates seamlessly with Elastic's Logstash, Beats and Kibana tools to create a more effective SIEM approach. Beginning at the bottom of the pyramid, empow enriches every security event with the attacker intent in the digestion level. All these enriched logs are stored in Elasticsearch, allowing analysts to conduct much more efficient investigations and forensics operations. In the middle of the pyramid i-SIEM applies cause & effect intelligence, which automatically correlates all classified events and prioritizes the real attacks and entities at real risks. At the top of the pyramid, empow utilizes the Kibana framework to clearly visualize these high risk attacks and entities, and allow easy drill down into the most relevant data. The overall solution provides a top-down analysis experience for identifying attacks, all without human generated rules.



Prioitize entities in real
risk and classify the related
threats (MITRE)

Cause & Effect analytics
automatically reduce noise
and prioritize real threats

Quick data onboaring via auto logs
classification using NLP, NTA,
and UEBA algorithms

# i-SIEM Benefits

| Today's SIEM Solutions | empow's i-SIEM |
|---|---|
| Long time to maturity – lengthy and expensive implementation process | Shortest route to a mature security posture |
| ⊗ Limited to out of the box basic security use cases | ✓ Wide coverage – automatically correlates security logs to identify advanced threats (no human generated rules required) |
| ⊗ Reactive, limited to known attack patterns | ✓ Proactive – powerful AI enables constant identification of new attack patterns |
| ⊗ No adaptive investigation and incident response functions | ✓ Automated investigation and response processes |
| ⊗ Flood the system with false positives | ✓ Reduces false positive rates by an average of at least 90% |
| ⊗ Complex to integrate with data-sources | ✓ Seamless data digestion based on empow's data classification technology |
| ⊗ Lack of out of the box general-purpose data and logs analysis techniques | ✓ Best in class data lake with full Elastic log analytics premium features and largest community enriching it |
| ⊗ High TCO – massive expert involvement, expensive and slow to implement | ✓ High ROI thanks to seamless integration, virtually no maintenance costs |

# Defense Models

empow's i-SIEM provides pre-built, customizable, defense models (called Security Apps) that allow the organization 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 Apps can be easily downloaded from empow's Security App Store 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 and account take over (ATO)**

**Intelligence gathering**

**Phishing and social attack campaigns**

**Insider threat**

**Data-leak**

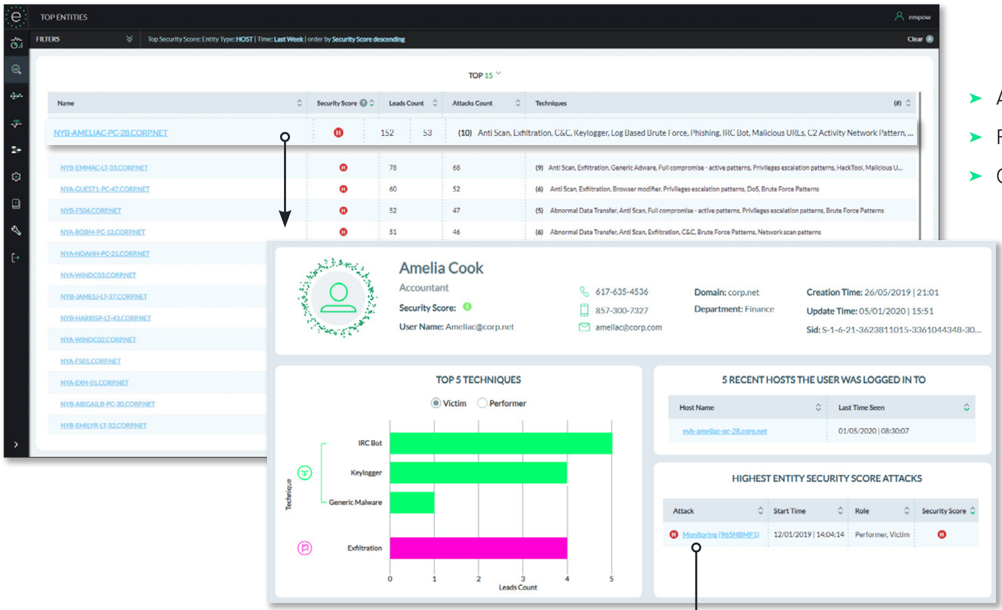
# User Experience - Working Top Down

i-SIEM turns the analyst's flow upside down. Instead of an army of analysts working their way through the mountain of logs from the bottom up, they can now work top down. The security analyst gets a small number of high risk entities, drills down into each suspicious entity, sees all the stages and information on that entity, understand the risk to the organization and is now able to act on it.

This flow provides three main benefits:

- Faster root-cause analysis, i.e., understanding the source of the attack (how it all started).
- Understand the full potential impact of the attack. For example how many other entities are infected by the same attack campaign, or the level of the attack spread within the organization.
- Fast and effective remediation actions, thanks to MITRE ATT&CK™ language.

## Real Time Monitoring of Prioritized Entities



TOP ENTITIES

FILTERS | Top Security Score: Entity Type: **HOST** | Time: **Last Week** | order by **Security Score descending** | Clear

TOP 15

| Name | Security Score | Leads Count | Attacks Count | Techniques (#) |
|---|---|---|---|---|
| NYB-AMELIAC-PC-28.CORP.NET | H | 152 | 53 | (10) Anti Scan, Exfiltration, C&C, Keylogger, Log Based Brute Force, Phishing, IRC Bot, Malicious URLs, C2 Activity Network Pattern, ... |
| NYB-EMMAC-LT-33.CORP.NET | H | 78 | 68 | (9) Anti Scan, Exfiltration, Generic Adware, Full compromise - active patterns, Privileges escalation patterns, HackTool, Malicious U... |
| NYA-GUEST1-PC-47.CORP.NET | H | 60 | 52 | (6) Anti Scan, Exfiltration, Browser modifier, Privileges escalation patterns, DoS, Brute Force Patterns |
| NYB-FS04.CORP.NET | H | 52 | 47 | (5) Abnormal Data Transfer, Anti Scan, Full compromise - active patterns, Privileges escalation patterns, Brute Force Patterns |
| NYA-BOBM-PC-12.CORP.NET | H | 51 | 46 | (6) Abnormal Data Transfer, Anti Scan, Exfiltration, C&C, Brute Force Patterns, Network scan patterns |
| NYA-NOAHH-PC-21.CORP.NET | | | | |
| NYA-WINDC03.CORP.NET | | | | |
| NYB-JAMESJ-LT-37.CORP.NET | | | | |
| NYB-HARRISP-LT-43.CORP.NET | | | | |
| NYA-WINDC02.CORP.NET | | | | |
| NYA-FS01.CORP.NET | | | | |
| NYA-EXH-01.CORP.NET | | | | |
| NYB-ABIGAILB-PC-30.CORP.NET | | | | |
| NYB-EMILYR-LT-32.CORP.NET | | | | |

Amelia Cook
Accountant
Security Score:
User Name: Ameliac@corp.net

617-635-4536
857-300-7327
ameliac@corp.com

Domain: corp.net
Department: Finance

Creation Time: 26/05/2019 | 21:01
Update Time: 05/01/2020 | 15:51
Sid: S-1-6-21-3623811015-3361044348-30...

5 RECENT HOSTS THE USER WAS LOGGED IN TO

| Host Name | Last Time Seen |
|---|---|
| nyb-ameliac-pc-28.corp.net | 01/05/2020 \| 08:30:07 |

HIGHEST ENTITY SECURITY SCORE ATTACKS

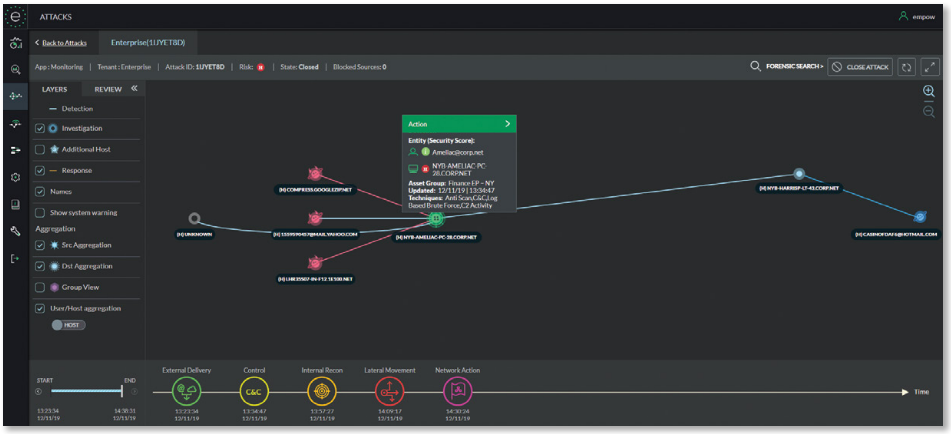
| Attack | Start Time | Role | Security Score |
|---|---|---|---|
| H Monitoring (965HBMF1) | 12/01/2019 \| 14:04:14 | Performer, Victim | H |

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

## Entity Card

- Entity's organizational context
- Impact analysis score

## Attack Story



ATTACKS

< Back to Attacks | Enterprise(1IJYET8D)

App : Monitoring | Tenant : Enterprise | Attack ID: 1IJYET8D | Risk: H | State: Closed | Blocked Sources: 0

LAYERS | REVIEW

— Detection
☑ Investigation
☐ Additional Host
☑ — Response
☑ Names
☐ Show system warning
Aggregation
☑ Src Aggregation
☑ Dst Aggregation
☐ Group View
☑ User/Host aggregation
HOST

Action
Entity (Security Score):
Ameliac@corp.net
NYB-AMELIAC-PC-28.CORP.NET
Asset Group: Finance EP – NY
Updated: 12/11/19 | 13:34:47
Techniques: Anti Scan,C&C,Log Based Brute Force,C2 Activity

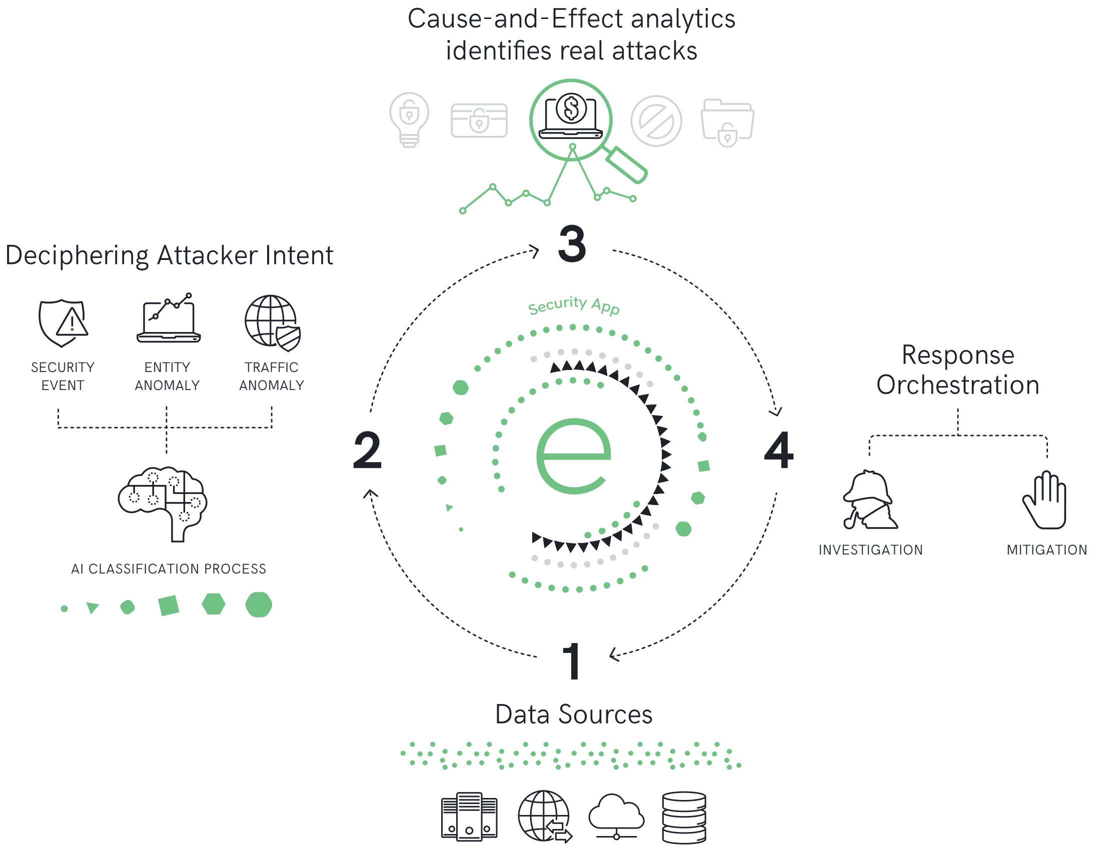
- Visualize time-based attack story
- Quick root-cause analysis
- Advise response types
- Enables forensic search & hunting

i-SIEM is seamlessly integrated into the organization's overall existing workflow incident response procedures and systems through pre-defined and customized alerts which allow to notify 3rd party security operation systems, including ticketing and case management solutions..

# How It Works

empow's i-SIEM collects and analyzes the IT data and actualizes the selected and customized defense models.The i-SIEM technology provides a constantly updated loop of detection, investigation and response.

The solution is made possible by proprietary patented AI technologies, which are strategically integrated into the following process:



### 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 zero 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.

# UEBA & NTA Engines

empow's i-SIEM comes with out-of-the-box UEBA (User Entity Behavioral Analytics) and NTA (Network Traffic Anomaly supported by empow's DPI network agents)  engines 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 empow's i-SIEM enables alerts that are automatically classified by attacker intent, with no correlation rules.

# Classification based on Threat Intelligence

The 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

# i-SIEM empowered by Elastic

Provides a shortcut to security maturity, and a SIEM that can be managed by less than one security analyst

Automatically identifies and mitigates advanced threats missed by single (siloed) tools - no rules required.

Proactive - powerful AI enables constant identification of new attack patterns.

Reduces noise by at least 90% and increases security operation effectiveness by 10x.

Provides ONE source for best in class searchable data lake (by Elastic) integrated with intent-based SIEM.

## Turn What You Have Into What You Need

e 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