empow

You have it in you.

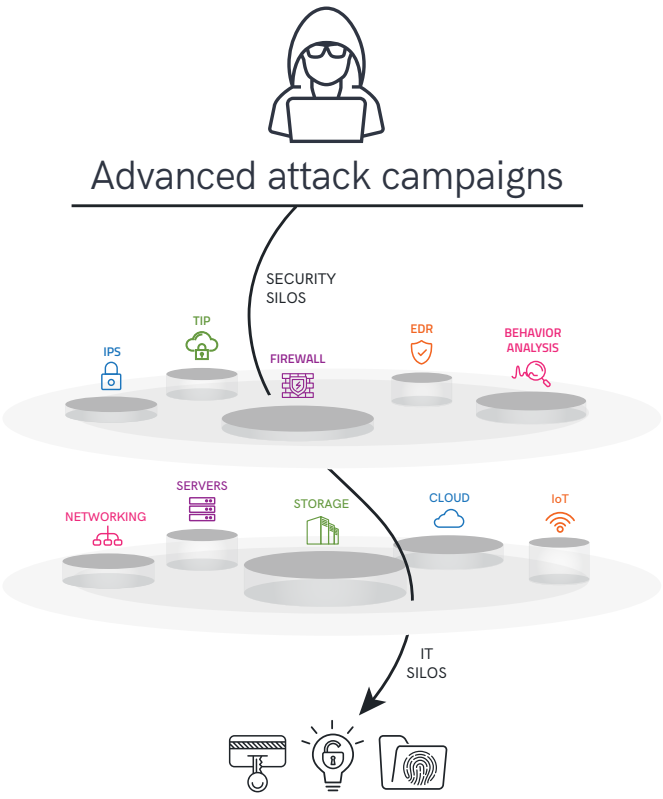
# The Challenges Today

Organizations deploy a variety of security tools, distributed across their different environments such as cloud, on-prem, end points and IOT, to protect their networks. In many cases they also invest in cyber operational tools such as Security Information and Event Management (SIEM), Threat Intelligence and Security Orchestration, Automation and Response (SOAR) tools.

Despite this massive investment, organizations still suffer from noisy, ineffective security platforms, because of the following issues:

### "Silos Syndrome"

The siloed nature of diverse technologies coupled with the dispersed nature of large organizations with many departments and a similarly dispersed Security Operations Center (SOC) makes it easy for information to fall through the cracks, giving potential attackers an opening into the network.




### Noise

Alert fatigue and noise, including from the security tools, SOAR and SIEM, prevent security teams from being able to detect and conduct prioritized and accurate response actions.

### Heavy Lifting

The need to manually create and maintain alerts rules, cross-correlations rules, and response workflow scripts (playbooks) puts a heavy ongoing burden on SOC teams, disrupting them from focusing on their real job - finding and preventing attacks.

### Pricing

Many SIEMs are priced according to ingestion data volume, which makes them vulnerable to cost-creep, making budgeting difficult and creating an unpredictable financial burden.

Security professionals who have implemented a SIEM platform and other response tools still need to provide a solution for these pain points. They are looking to improve the performance and lower the cost of their SIEM, and to have greater visibility into their different security products and their performance.

# About i-XDR

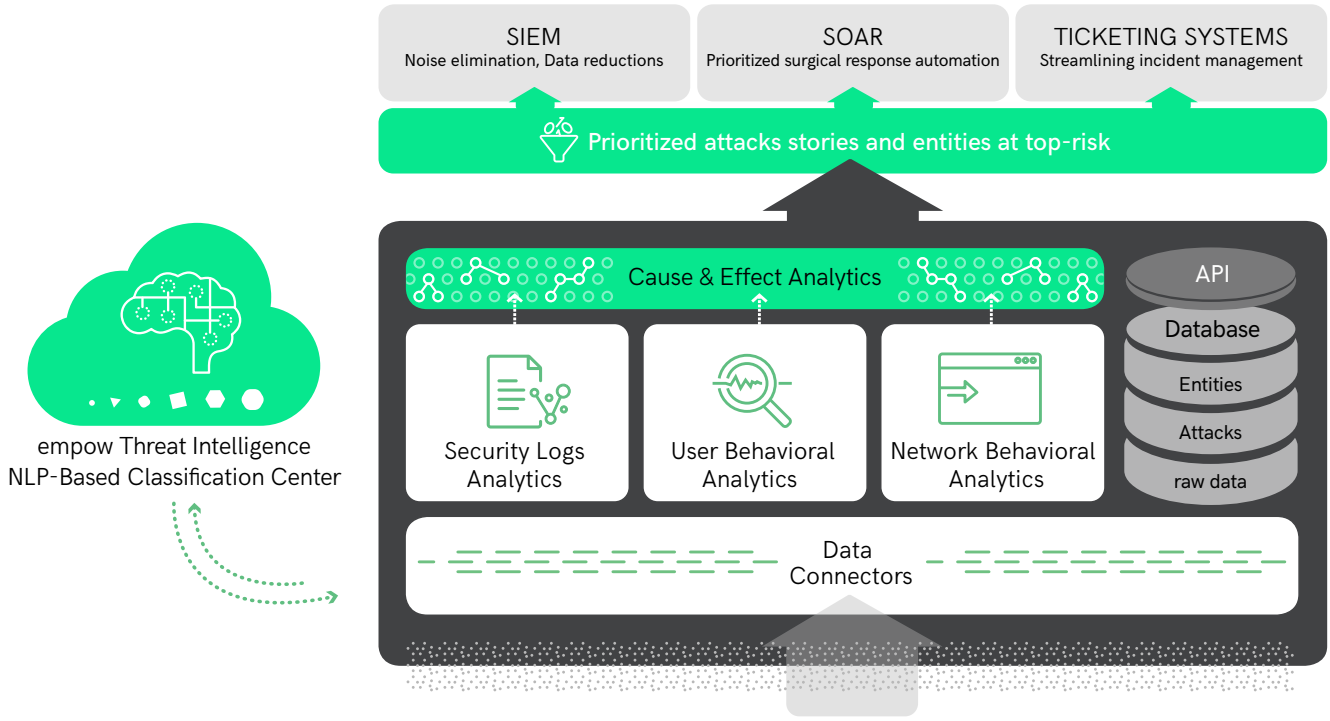
The Extended Detection and Response (XDR) approach extends protection beyond endpoints to provide detection and response across broader systems and networks.  These include cloud services, on-premise data centers, and Internet of Things (IoT) networks – basically pretty much all of the security tools active in the organization, including the SIEM.

empow's i-XDR is an intent-based Extended Detection and Response (XDR) platform that gets your entire security operations to run faster and better. By automatically classifying and correlating network activity, user activity and security telemetry data, it reduces the ingestion and research burden, saving valuable time and money.

i-XDR is based on empow's patented Artificial Intelligence (AI) and Natural Language Processing (NLP) algorithms, reinforced with User Entity Behavior Algorithms (UEBA), Network Traffic Analysis (NTA), and Threat Intelligence engines, to enable automated classification and prioritization of threats and remediation processes. The unique automated technology also enables the system to find out attacker "intent" before the attack is carried out, enabling a proactive, predictive security.

i-XDR analyzes, prioritizes and delivers a small number of truly at-real-risk entities and attacks to the organization's SIEM, SOAR or other orchestration tools, lowering cost, increasing speed and improving performance. Alternately an organization can choose to work directly via i-XDR's operational dashboards.

# How i-XDR works



## Data Connectors

empow's data connectors collect all types of IT data from a wide diversity of endpoint & network-based security tools, user and network activity logs, including on-prem & cloud data sources.

## AI-Based Analytical Modules:

### Security Logs Analytics

The NLP-based security logs analytics processes all your security logs, enriches them with empow's threat intelligence information and use our proprietary NLP engines to classify these logs into groups of potential attack behaviors.

### User Behavioral Analytics

User activity logs are processed by empow's user behavioral analytics module, which establishes normal behavioral profile patterns and flags deviations which reflect potential attack behaviors.
Read more in our **UEBA white paper.**

### Network Traffic Analytics

empow's DPI network sensors feed the network traffic analytics module, which learns the normal traffic patterns between hosts within the organization and flags anomalies that reflects both unknown and unknown potential attack behaviors. Read more in our **NTA white paper**.

### empow Threat Intel NLP- Based Threat Classification Center

The NLP-based threat classification center continuously collects threat intelligence from multiple commercial and open threat centers, enriches the information analyzed by the analytics module and uses the power of NLP to classify these modules' output into potential attack techniques and tactics – using one language of ATT&CK.
Read more in our **AI white paper.**

### Cause & Effect Module

This module incorporates proprietary algorithms that process the outputs of all analytics, automatically identifies potential root-cause and attack next steps in order to cluster the logs into only a few real attack stories. The result is a timeline of real attacks and prioritized entities that are at top risk.

# i-XDR makes your existing security tools better, faster and more efficient.

## Here's how i-XDR integrates with your existing security tools:

### SIEM

Significantly reduces the cost of your data consumption-based SIEM license.

Streamlines the SOC operations of your existing SIEM, reduces time to detect, investigate & respond.

### Incident Management Systems

No more hundreds of tickets to handle. Improves the efficiency of your existing ticketing systems by issuing and updating the most relevant and accurate security tickets.

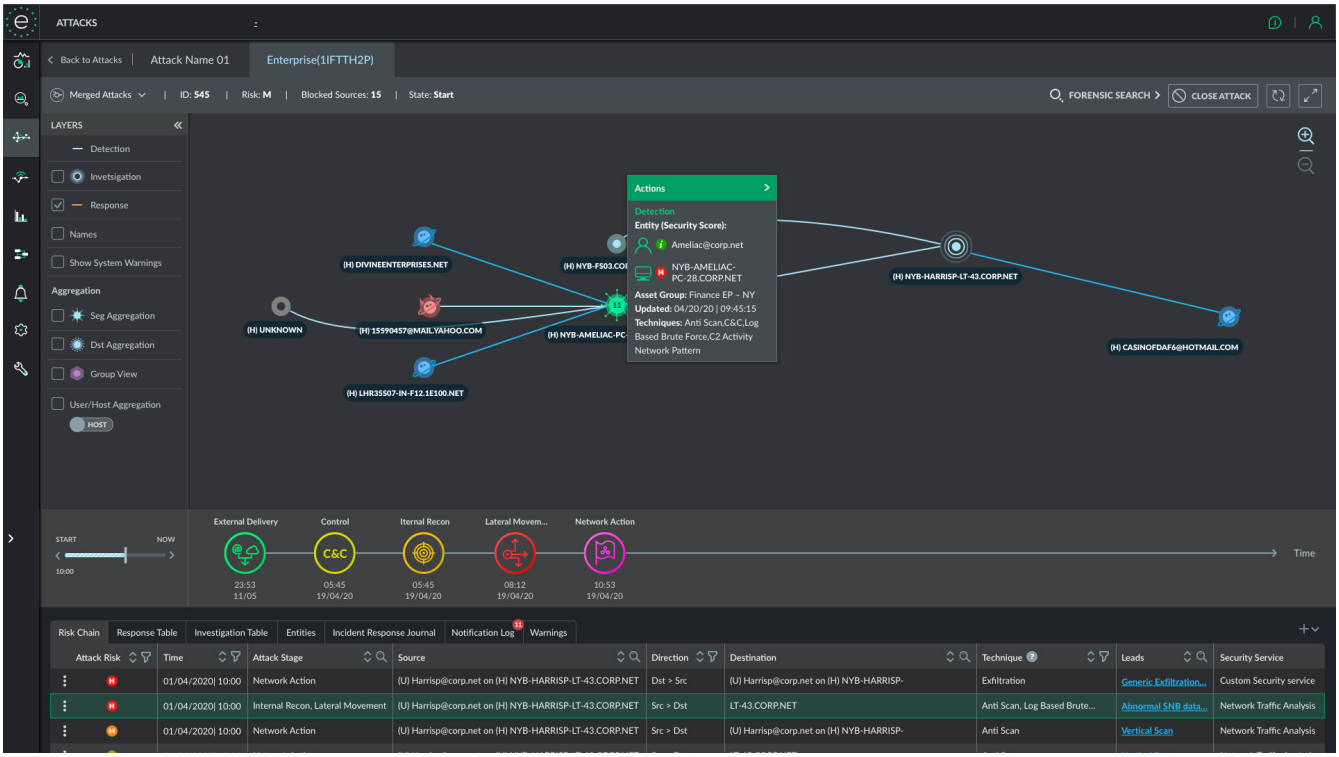
### SOAR

Provides immediate and accurate response by triggering your existing SOAR playbooks only for entities that are at top risk, allowing a smaller team to handle more incidents.

### Investigation APIs

Rich APIs allow your SOC to integrate with the system's data for in-depth forensics investigation and automation use cases.

## Security analysts love our dashboard!



empow
You have it in you.

Tel: +1-877-647-4361
30 Newbury Street, 3rd Floor
Boston, MA 02116, United States

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

www.empow.co
info@empow.co