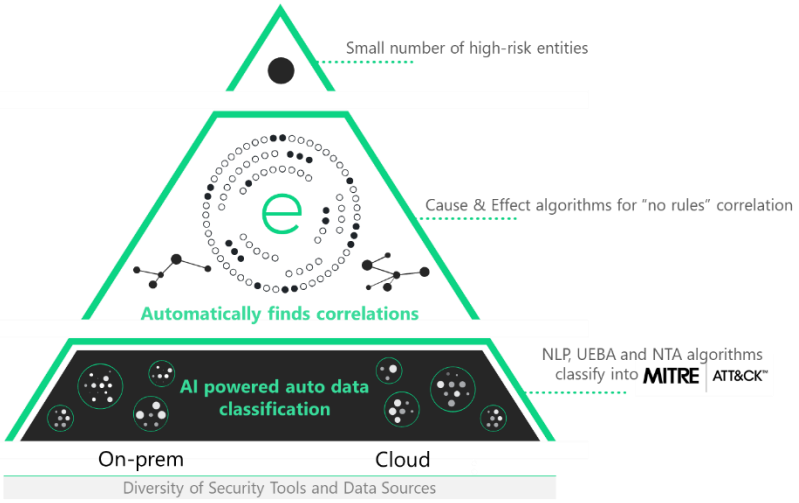
Data Source Ingestion with AWS

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering fully featured services in data centers globally. As organizations become more agile, and innovate faster on this platform, it has become even more challenging to protect entities, users, and data from attack.

The flexibility of the platform can sometimes generate huge amounts of noise and false positives in data flows, making this even more difficult. By using the empow i-SIEM's automated data feeds, security analysts can focus only on those few entities that pose a real potential of harm or are at real risk of compromise. Moving from a historical review to predictive analytics allows empow to streamline and prioritize remediation efforts, saving money and time.

empow leverages the Elastic Stack



Using proprietary Artificial Intelligence (AI) algorithms based on Natural Language Processing (NLP) and Adaptive Anomaly Behavior detection engines, empow automatically classifies and normalizes the data and logs into behavioral groups of potential threats, creating a unified language using the MITRE ATT&CK™ framework for investigation and correlation. Using the proprietary, patented cause-and-effect algorithms (a key technology only available through empow), i-SIEM autonomously identifies "connections" between the groups of potential threats, allowing the system to correlate (and triage) large volumes of data, eliminate noise and prioritize only what is really important. All of this is done automatically, out-of-the-box with no need to create and maintain correlation rules nor threshold alerts.

The goal for AWS security integration is to help analysts focus on true potential threat alerts without requiring an extensive technical integration effort.

Today, most AWS investigation and hunting tools require security analysts to manually investigate huge amounts of data – requiring lots of time and money. In fact, no matter how many experts are hired, no matter how experienced they are, or how much money

TECH NOTE

empow cyber security
129 Newbury Street
Boston, MA 02116 USA

www.empow.co
info@empow.co
+1-877-647-4381

is spent on resolving this problem, without AI, NLP, and automated correlation technology, there will always be delayed detection, minimal investigation, and manual resolution, making threat responses ineffective.

Identifying Attack Vectors

As enterprise organizations move to the cloud, one of their main challenges is to enforce holistic security monitoring which will allow them to identify threats that are traversing these boundaries. In general, there are three main threat vector categories:

- Threats that originate **at the on-prem organization** level (employees' computers) and then infect **the organization's cloud assets** (in some cases multi-cloud providers).
- Threats that originate **at the organization's cloud assets** and infect **the organization's** employees' computers.
- Threats that originate **from employees who are infected at home**, or during travel, and through various lateral movements infect both **the cloud and on-prem organizational assets**.

The empow i-SIEM's UEBA, NTA and cause-and-effect correlation algorithms were designed to provide visibility, detection and investigation of these threat scenarios.

This ability to classify and integrate both on-prem signals as well as cloud-based signals into one language of attack behaviors (e.g., MITRE attach techniques) and to correlate these behaviors in order to find and prioritize persistent threats without human generated rules is unique to empow (bypassing the need for correlation, triage and root cause analysis rules).

Following are many of the security use cases for cloud-based workload activity signals, referring specifically to AWS Identity and Access Management (IAM) and GuardDuty via CloudTrail (analyzed by empow's UEBA engines), and virtual private cloud (VPC) flows (analyzed by empow's NTA engines), and which are automatically correlated via empow's cause-and-effect algorithms with other signals that the i-SIEM digests (e.g., security alerts, on prem or cloud based):

Using AWS related events from source to security

Feed	empow Use Case	Attack Technique or Tactic
IAM	Brute force and password guessing attempts	Credential access
IAM	Impossible user logins (location-based, time-based)	Privilege escalation
IAM	New service or new account	Persistence and privileges escalation
IAM	New user or new role	Account manipulation, Persistence
IAM	Updating account info	Account manipulation, Persistence
VPC	Network scans and service scans	Discovery
VPC	Service brute force	Credential access
VPC	New flow anomalies	Data leak, communication with malicious sites, lateral movement
VPC	Drop point behavior	Data leak behavior
VPC	Abnormal data transfers	Data leak behavior
GuardDuty	Backdoor	Command & Control activities
GuardDuty	Crypto currency	Misuse of resources
GuardDuty	Penetration Test	Technical & vulnerability information gathering (pre-attack)
GuardDuty	Persistence	Persistence techniques (e.g., abnormal network configuration settings)
GuardDuty	Privilege Escalation	Privilege Escalation
GuardDuty	Recon	Network service scanning
GuardDuty	Stealth	Anonymity services
GuardDuty	Trojan	Various trojan techniques (classified by empow's i-SIEM)

The data feeds and techniques listed above are automatically classified, normalized by empow and correlated real-time with other signals in order to provide a clear picture of the attack story. This prioritizes the most relevant entities that are currently compromised or are at future risk of compromise without manual effort nor custom programming.

Please contact empow for further information or technical documentation on this capability.

empow cyber security
129 Newbury Street
Boston, MA 02116 USA

www.empow.co
info@empow.co
+1-877-647-4381