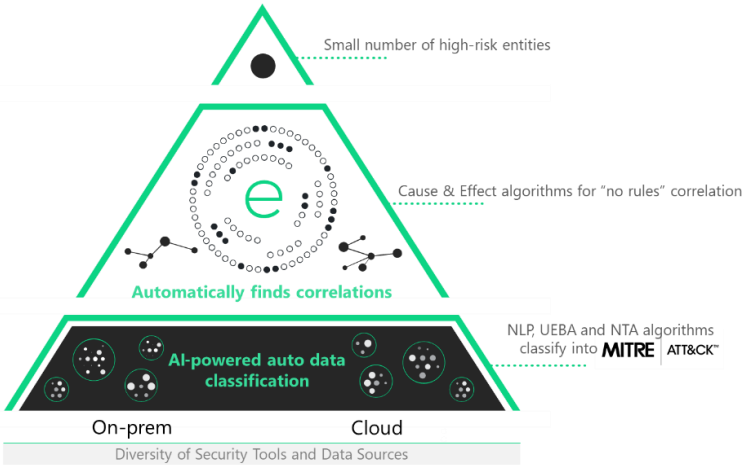
empow Data Source Ingestion with Azure: Visibility and Control Over Your Cloud Environment

Azure cloud is one of the world's most comprehensive and broadly adopted cloud platforms, 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 attacks.

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 on 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 it 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 from 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 or threshold alerts.

The goal for Azure and O365 integration is to help analysts focus on true potential threat alerts, without requiring an extensive technical integration effort.

TECH NOTE

empow cyber security
129 Newbury Street
Boston, MA 02116 USA

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

Today, most Azure investigation and hunting tools (Azure Microsoft Security Center) require security analysts to manually investigate huge amounts of data – which translates into lots of time and money. In fact, no matter how many experts are hired, no matter how experienced they are, or how much money is spent 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 traverse 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 behavior (e.g., MITRE ATT&CK™ 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 and email security, referring specifically to Azure Cloud & O365 Services APIs, which are automatically classified and correlated via empow's NLP and cause-and-effect algorithms with other signals that the i-SIEM digests (e.g., on prem originated security alerts, threat intelligence and others):

Using Azure Cloud and O365 Related Events from Source to Security

Feed	Use Cases Examples	Attack Tactics and Techniques
O365 ATP	Detection of phishing, social engineering, and malware delivery.	**Initial Access:** Drive-by Compromise, Spearphishing Link, Spearphishing Attachment **Execution**: Various trojan software (classified by empow's i-SIEM)
Azure Active Directory / O365	Detection of malicious account access and account manipulation activities, that can be result of identity theft, ATO and insider activity.	**Credential Access**: Steal Application Access Token, Account Manipulation, Valid Accounts, Account Access Removal
Azure Application Gateway	Detection of malicious activities on external facing applications and servers that can result with DoS, Data-theft and full compromise.	**Initial Access**: Exploit Public-Facing Application, Drive-by Compromise **Discovery**: Network Service Scanning **Impact:** Denial of Service
Azure Security Center	Detection of malicious account access and account manipulation activities, that can be result of identity theft, ATO (account take over) and insider activity.	**Credential Access, Privileges Escalation**: Account Manipulation, Brute Force, Credential Dumping, Valid Account
	Detection of attackers and insiders trying to get stronghold on computers in the network in order to gather information, manipulate and eventually steal data	**Discovery**: Network Service Scan **Persistence**: Modify Existing Service, Implant Container Image, Create Account **Privileges Escalation**: Valid Account **Lateral Movement**: Pass the Hash
	Detection of attackers trying to council their tracks	**Defense Evasion**: Bypass User Account Control, Revert Cloud Instance
	Detection of attempts to steal and exfiltrate data	**Exfiltration**: Scheduled Transfer **Collection**: Email Collection **Command and Control**
	Ransomware detection	**Impact**: Data Encrypted for Impact, Ransomware
	Detection of malware running in the network	**Execution**: Various trojan software (classified by empow's i-SIEM)

The data feeds and techniques listed above are automatically classified, normalized by empow's i-SIEM and correlated in 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 or custom programming.