Microsoft

Microsoft Advanced Threat Analytics

How it works

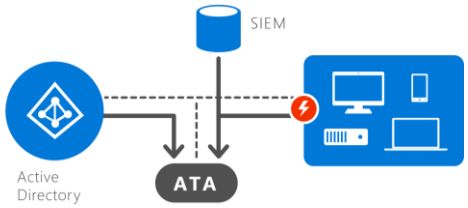
Microsoft Advanced Threat Analytics (ATA) provides a simple and fast way to understand what is happening within your network by identifying suspicious user and device activity with built-in intelligence and providing clear and relevant threat information on a simple attack timeline.

Microsoft Advanced Threat Analytics leverages deep packet inspection technology, as well as information from additional data sources (SIEM and AD) to build an Organizational Security Graph and detect advanced attacks in near real time.

The ATA system continuously goes through four steps to ensure protection:

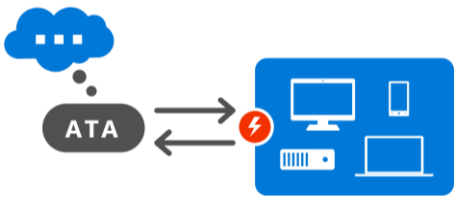
Step 1: **Analyze**

After installation, by using pre-configured, non-intrusive port mirroring, all Active Directory-related traffic is copied to ATA while remaining invisible to attackers. ATA uses deep packet inspection technology to analyze all Active Directory traffic. It can also collect relevant events from SIEM (security information and event management) and other sources.



Step 2: **Learn**

ATA automatically starts learning and profiling behaviors of users, devices, and resources, and then leverages its self-learning technology to build an Organizational Security Graph. The Organizational Security Graph is a map of entity interactions that represent the context and activities of users, devices, and resources.

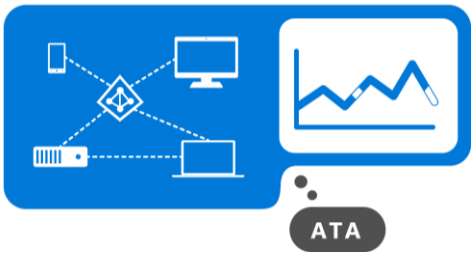


Step 3: **Detect**

After building an Organizational Security Graph, ATA can then look for any abnormalities in an entity's behavior and identify suspicious activities—but not before those abnormal activities have been contextually aggregated and verified.

ATA leverages years of world-class security research to detect known attacks and security issues taking place regionally and globally.

ATA will also automatically guide you, asking you simple questions to adjust the detection process according to your input.



Step 4: **Alert**

While the hope is that this stage is rarely reached, ATA is there to alert you of abnormal and suspicious activities. To further increase accuracy and save you time and resources, ATA doesn't only compare the entity's behavior to its own, but also to the behavior of other entities in its interaction path before issuing an alert. This means that the number of false positives are dramatically reduced, freeing you up to focus on the real threats.

At this point, it is important for reports to be clear, functional, and actionable in the information presented. The simple attack timeline is similar to a social media feed on a web interface and surfaces events in an easy-to-understand way.

ATA detects:

Security issues

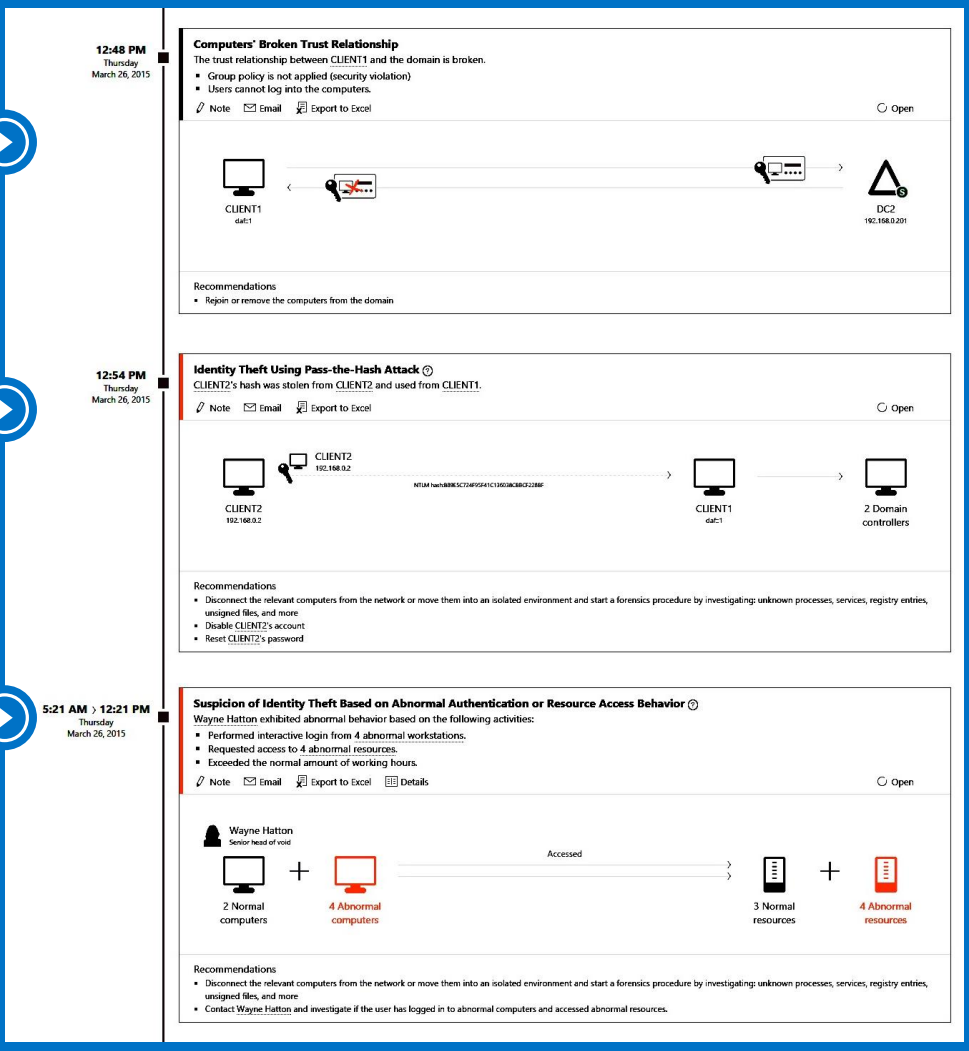
(broken trust, weak protocols, known protocol vulnerabilities)

Malicious attacks

(Pass the Ticket, Pass the Hash, forged PAC, Reconnaissance, BruteForce)

Abnormal behavior

(anomalous logins, unknown threats, password sharing, lateral movement, and more)



For more information, please go to www.microsoft.com/ata

For trying and evaluating ATA, please visit
http://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics