KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | August 2016

Microsoft Advanced Threat Analytics

Microsoft Advanced Threat Analytics combines deep packet inspection with Active Directory and SIEM integration to build an Organizational Security Graph and identify suspicious user and device activity within corporate networks.

by **Alexei Balaganski**
ab@kuppingercole.com
August 2016

Content

Related Research

Advisory Note: Real Time Security Intelligence – 71033

Executive View: Microsoft Azure Active Directory – 71550

Executive View: Microsoft Azure RMS – 70976

1 Introduction

Microsoft is a multinational technology company headquartered in Redmond, Washington, USA. Founded in 1975, it has risen to dominate the personal computer software market with MS DOS and Microsoft Windows operating systems. Since then, the company has expanded into multiple markets like desktop and server software, consumer electronics and computer hardware, mobile devices, digital services and, of course, the cloud. Microsoft is the world's largest software company and one of the top corporations by market capitalization.

In 2008, the company entered the cloud computing market with their Azure platform, and since then cloud services have been one of the primary drivers in Microsoft's own digital transition from manufacturing towards becoming a global digital service provider. Currently, Microsoft's cloud platform provides a full stack of services ranging from compute and infrastructure to data storage, mobile and IoT device management, and, last but not least, identity. Azure is one of the global leaders in the cloud infrastructure market, second only to Amazon's AWS.

Although Microsoft's long-term strategy undoubtedly is to become primarily a cloud provider, it is also quite obvious that for most enterprises going fully cloud-based will not be a feasible option in the foreseeable future. For many reasons, including technical challenges, regulatory compliance, and massive burdens of legacy applications, most companies have to opt for hybrid deployments for the present time, combining on-premises and cloud infrastructures. With Microsoft itself being a de facto leader in enterprise identity management with Active Directory, it is understandable that the company has a strong focus on various hybrid cloud solutions.

This also explains why Advanced Threat Analytics (ATA), a completely on-premises product, is developed by Microsoft's Cloud division and is being offered as a part of Microsoft Enterprise Mobility + Security, a solution comprising both products like Microsoft Cloud App Security, which are purely targeted at cloud services, as well as solutions like InTune or Azure Information Protection, which address the full spectrum of challenges of a hybrid deployment.

Like several other products from the suite, Microsoft Advanced Threat Analytics is based on an acquisition. In 2014, Microsoft acquired Aorato, an Israel-based startup company specializing in hybrid cloud security solutions. Aorato's behavior detection methodology, aptly named Organizational Security Graph, provides non-intrusive collection of network traffic, event logs and other data sources in an enterprise network and then, using behavior analysis and machine learning algorithms, detects suspicious activities, security issues and cyber-attacks. In August 2015, the new product was officially launched as a part of Microsoft's portfolio and the most recent update has been released in June 2016.

Being able to correlate both real-time and historical events (from existing SIEM tools) and using Big Data analytics technology to reduce the number of false positives, the product fully aligns with KuppingerCole's definition of a Real-Time Security Intelligence solution. As a part of the Enterprise Mobility + Security it serves an important purpose of protecting on-premises networks from both internal and external threats and thus both simplifying and strengthening a company's security posture.

2 Product Description

Microsoft Advanced Threat Analytics (ATA) is a security monitoring solution that monitors and analyzes network traffic, event logs and data from additional data-sources to detect both known malicious activities and suspicious entity (that is, any user, device or resource) behavior to identify advanced targeted attacks or insider threats on corporate networks.

The solution can be deployed as an out of band solution by using port mirroring, thus requiring no changes to an existing infrastructure. Additionally, it can be deployed directly on domain controllers, thus removing the overhead of additional servers. Naturally, the product supports both physical and virtualized deployments.

A typical deployment consists of an **ATA Center**, which serves as the centralized data storage and correlation engine and provides the management console, and a number of **ATA Gateways** deployed on standalone servers. After deployment, the product automatically starts analyzing the network traffic copied by port mirroring (thus remaining invisible to attackers). Alternatively, the product can utilize **ATA Lightweight Gateways** deployed directly on domain controllers – this can provide significant savings on hardware, but won't achieve the same level of transparency and isolation as using dedicated gateways.

To further improve its detection capabilities, the product supports the collection of identity-related events from the Windows Event Logs. This requires a one-time configuration of the domain controller. Additionally, it supports integration with leading SIEM solutions like IBM QRadar, HP ArcSight, RSA Security Analytics and Splunk. This includes both receiving security events from these products over a standard syslogd interface and sending events back to a SIEM for each detected suspicious activity.

Since the product analyzes all authentication and authorization events, it's able to monitor all assets communicating with the corporate Active Directory regardless of their location, including mobile devices beyond the corporate perimeter. Based on Aorato's proprietary technology, Advanced Threat Analytics can instantly identify a large number of known malicious attacks, such as Pass-the-Ticket, Pass-the-Hash, Golden Ticket and others. Additionally, it identifies various security issues within the network, such as weak protocols, known vulnerabilities and broken trust. However, using behavior analytics technologies, the product can identify previously unknown suspicious activities as well: anomalous logins, password sharing, lateral movements and so on.

To achieve that, the solution first needs to learn and profile behavior patterns of users, devices and other resources. After the initial analysis, an Organizational Security Graph is created, which contains a full map of interactions between all entities. This graph provides the "normal" baseline to detect behavioral anomalies and other suspicious activities. As typical for Real-Time Security Intelligence solutions, there is no need to define any rules or adapt the product to organizational changes. Again, following the RTSI definition, the solution dramatically reduces the number of false positives, providing a list of a relatively few highly-probable suspicious activities, clearly ranked by severity.

Where the product does differ from many other RTSI solutions on the market is how the correlation engine can directly incorporate the results of multiple algorithms looking for advanced attacks and security risks into its analysis. Thus, it is not simply blindly looking for anomalies, but for meaningful

signs of known attack techniques. This dramatically improves overall detection quality, and the solution can reliably identify an advanced attack regardless of the specific malware tool. In a sense, Microsoft ATA combines and extends the advantages of both traditional signature-based security tools and new behavior analytics solutions. As the product is integrated into Microsoft Update, new releases are deployed automatically, bringing new detection methods and improvements for existing ones transparently for administrators.

It's worth noting that in the standard configuration, the product is collecting a substantial amount of anonymized telemetry information about detected suspicious activities, which is sent to Microsoft to improve future detection capabilities. No sensitive information like computer names, user names, and IP addresses is collected, however, and customers have the option to disable this feature completely if needed.

The **Advanced Threat Analytics Console** provides a web-based management interface for the solution. It shows a quick overview of all detected suspicious activities, allows security analysts to drill into details of any entity in the environment, perform investigation of the suspicious activities, show alerts and notifications and, of course, provides configuration and service health monitoring functions.

The key element of the console is the Attack Timeline, which shows a chronological list of suspicious activities, with key information about the entities and assets involved, event severity, as well as the details of the attack. Every suspicious activity can be reviewed and, if needed, marked as a resolved or dismissed. Seasoned experts can access all raw security data directly in the product's database engine. For certain types of suspicious activities, the product may even ask for additional context: for example, whether remote execution is allowed on a particular computer. A positive answer will influence the organizational security graph and similar activities from the same computer will no longer generate alerts.

In addition to the timeline, the console can display profiles for each user and device in the organizational security graph, showing such information as recently accessed resources or logged in devices, group membership, login history and past suspicious activities. A search bar provides quick access to any resource known to the system.

All newly detected suspicious activities can be automatically forwarded to a SIEM tool or generate email alerts. Each alert includes a direct link to a specific event in the attack timeline. Unfortunately, there are no additional settings available – the product will generate alerts for all activities regardless of their source or criticality.

Overall, Microsoft Advanced Threat Analytics is a perfect example of a Real-Time Security Intelligence solution with a background in the field of cybersecurity. It's focused on detection of several specific kinds of internal and external threats, and, as opposed to products evolving from traditional SIEMs, is much leaner and easier to deploy. It's also clearly more targeted towards business-oriented users than security forensic experts. By offering easy deployment without a manual training phase, as well as a clean and simple user interface with limited configuration options, it's especially suitable for smaller organizations.

However, by focusing on a specific area of information security – corporate identity infrastructure – the solution provides a valuable addition to the multi-layer corporate security architecture of any enterprise, especially important for companies with extensive hybrid cloud deployments.

3 Strengths and Challenges

Microsoft Advanced Threat Analytics provides a simple and convenient solution for identifying suspicious user and entity activities in corporate networks based on non-intrusive monitoring of activities and behavior. Evolving from a highly specialized network security tool, it utilizes machine learning algorithms and user and entity behavior profiling to reduce a large number of security events to a manageable list of suspicious activities, dramatically reducing administration effort and making the solution usable even for non-technical users.

However, a narrow focus on data collection from Active Directory servers means that the product is definitely not a replacement for a full-featured SIEM-based Security Operations Center. It should not be deployed as a standalone solution, but integrated into an existing multi-layer security infrastructure.

Although a strictly on-premises product, Microsoft Advanced Threat Analytics plays an important part in the company's cloud-delivered Enterprise Mobility + Security solution set.

Strengths	Challenges
• Integrated solution detecting security issues, malicious attacks and suspicious activities • Unique Organizational Security Graph technology • Transparent non-intrusive monitoring across internal and external assets • Bidirectional integration with leading SIEM solutions • Easy, flexible deployment, automated upgrades • Innovative user-friendly interface	• As a standalone product, not a replacement for traditional security tools • Limited forensic analysis capabilities • No filtering options for alerting

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com