Advanced Threat Analytics

@directorcia

http://about.me/ciaops

Sobering statistics

243

The average number of days that attackers reside within a victim's network before detection

76%

of all network intrusions are due to compromised user credentials

$500B

The total potential cost of cybercrime to the global economy

$3.5M

The average cost of a data breach to a company

The frequency and sophistication of cybersecurity attacks are getting worse.

Changing nature of cyber-security attacks

Today's cyber attackers are:

- Compromising user credentials in the vast majority of attacks
- Using legitimate IT tools rather than malware – harder to detect
- Staying in the network an average of eight months before detection
- Costing significant financial loss, impact to brand reputation, loss of confidential data, and executive jobs

Changing nature of cyber-security attacks

Today's cyber attackers are:

- Compromising user credentials in the vast majority of attacks
- Using legitimate IT tools rather than malware – harder to detect
- Staying in the network an average of eight months before detection
- Costing significant financial loss, impact to brand reputation, loss of confidential data, and executive jobs

Changing nature of cyber-security attacks

Today's cyber attackers are:

- Compromising user credentials in the vast majority of attacks
- Using legitimate IT tools rather than malware – harder to detect
- Staying in the network an average of eight months before detection
- Costing significant financial loss, impact to brand reputation, loss of confidential data, and executive jobs

Changing nature of cyber-security attacks

Today's cyber attackers are:

- Compromising user credentials in the vast majority of attacks
- Using legitimate IT tools rather than malware – harder to detect
- Staying in the network an average of eight months before detection
- Costing significant financial loss, impact to brand reputation, loss of confidential data, and executive jobs

The problem

Traditional IT security tools are typically:

Complex

Initial setup, fine-tuning, creating rules and thresholds/baselines can take a long time.

Prone to false positives

You receive too many reports in a day with several false positives that require valuable time you don't have.

Designed to protect the perimeter

When user credentials are stolen and attackers are in the network, your current defenses provide limited protection.

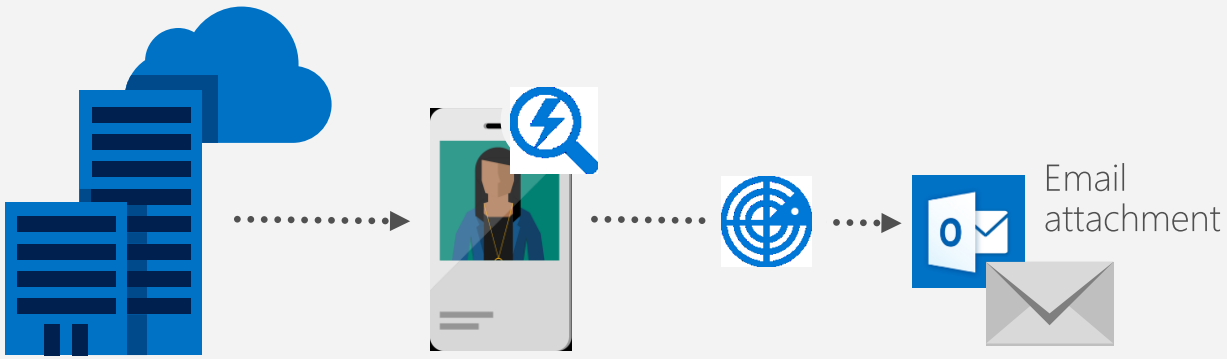
Introducing Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks *before* they cause damage

Comparison:

- **Credit card** companies monitor cardholders' behavior.
- If there is any abnormal activity, they will notify the cardholder to verify charge.

Microsoft Advanced Threat Analytics brings this concept to IT and users of a particular organization



Introducing Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks *before* they cause damage

Behavioral Analytics

Detection for known attacks and issues

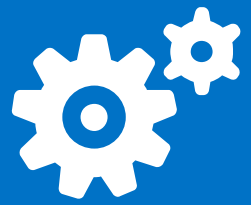
Advanced Threat Detection

Advanced Threat Analytics Benefits

Detect threats fast with Behavioral Analytics

No need for creating rules, fine-tuning or monitoring a flood of security reports, the intelligence needed is ready to analyze and self-learning.

Adapt as fast as your enemies



ATA continuously learns from the organizational entity behavior (users, devices, and resources) and adjusts itself to reflect the changes in your rapidly-evolving enterprise.

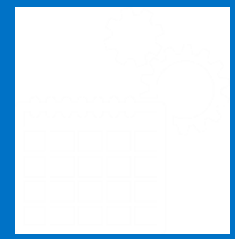
Focus on what is important fast using the simple attack timeline

The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving you the power of perspective on the "who-what-when-and how" of your enterprise.

Reduce the fatigue of false positives

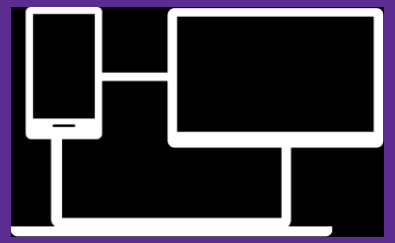
Alerts only happen once suspicious activities are contextually aggregated, not only comparing the entity's behavior to its own behavior, but also to the profiles of other entities in its interaction path.

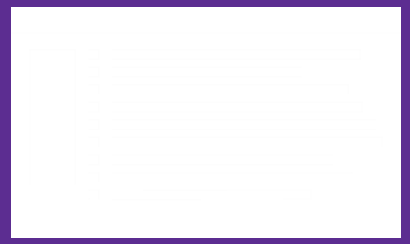
Prioritize and plan for next steps



For each suspicious activity or known attack identified, ATA provides recommendations for the investigation and remediation.

Key features





Mobility support

- Witnesses all authentication and authorization to the organizational resources within the corporate perimeter or on mobile devices

Integration to SIEM

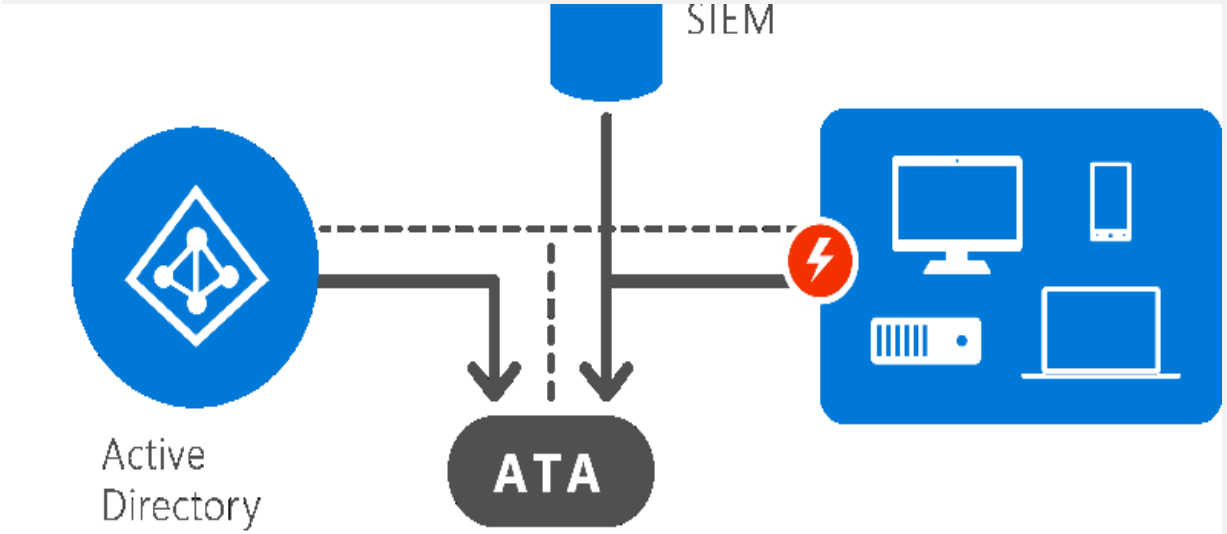
- Works seamlessly with SIEM
- Provides options to forward security alerts to your SIEM or to send emails to specific people

Seamless deployment

- Functions as an appliance hardware or virtual
- Utilizes port mirroring to allow seamless deployment alongside AD
- Does not affect existing network topology

How Microsoft Advanced Threat Analytics works

1 Analyze

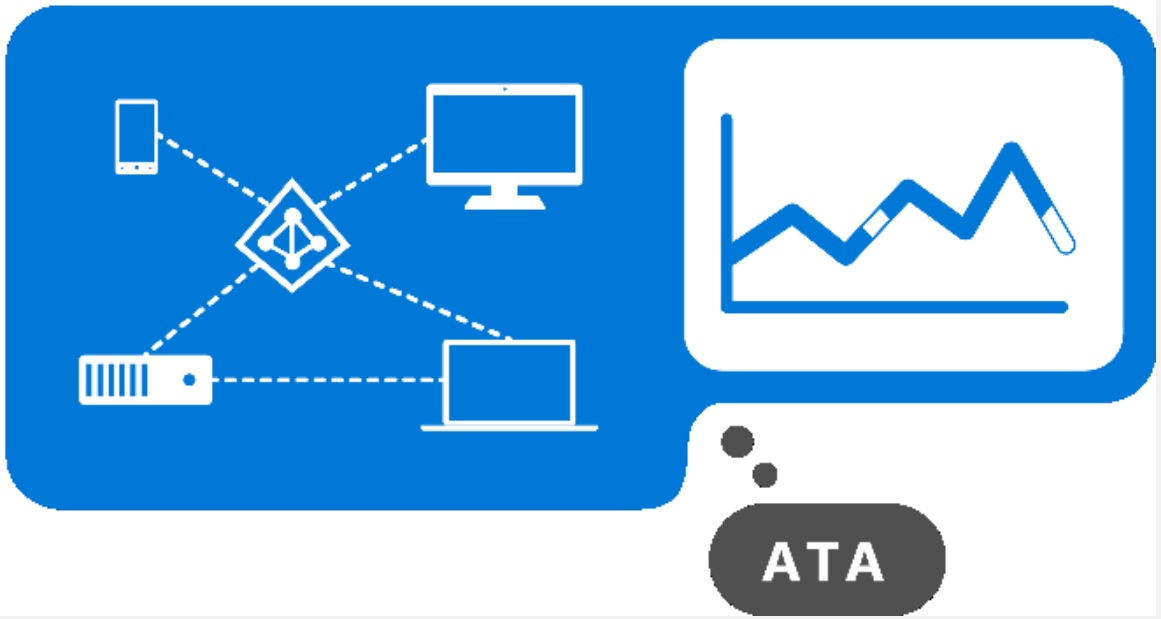


After installation:

- Simple non-intrusive port mirroring configuration copies all AD-related traffic
- Remains invisible to the attackers
- Analyzes all Active Directory traffic
- Collects relevant events from SIEM and other sources

How Microsoft Advanced Threat Analytics works

2 Learn



ATA:

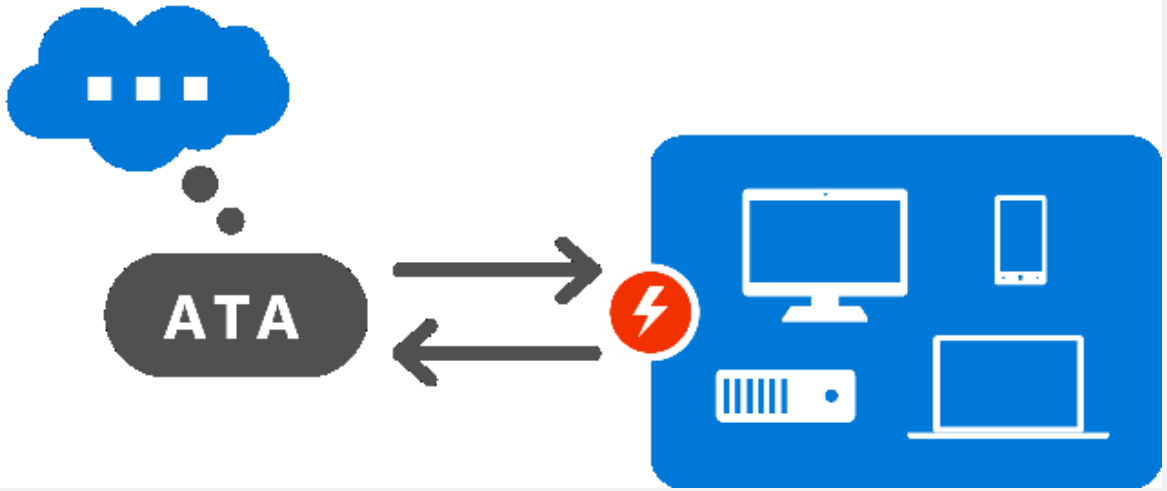
- Automatically starts learning and profiling entity behavior
- Identifies normal behavior for entities
- Learns continuously to update the activities of the users, devices, and resources

What is entity?

Entity represents users, devices, or resources

How Microsoft Advanced Threat Analytics works

3 Detect



Microsoft Advanced Threat Analytics:

- Looks for abnormal behavior and identifies suspicious activities
- Only raises red flags if abnormal activities are contextually aggregated
- Leverages world-class security research to detect known attacks and security issues (regional or global)

ATA not only compares the entity's behavior to its own, but also to the behavior of entities in its interaction path.

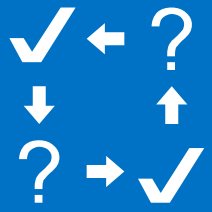
How Microsoft Advanced Threat Analytics works

4 Alert

ATA reports all suspicious activities on a simple, functional, actionable attack timeline

ATA identifies

- Who?
- What?
- When?
- How?

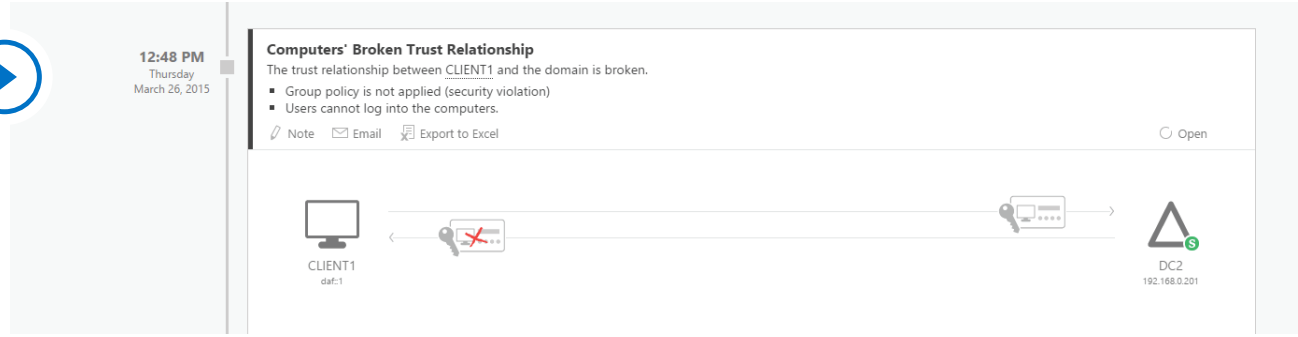


For each suspicious activity, ATA provides recommendations for the investigation and remediation.

How Microsoft Advanced Threat Analytics works

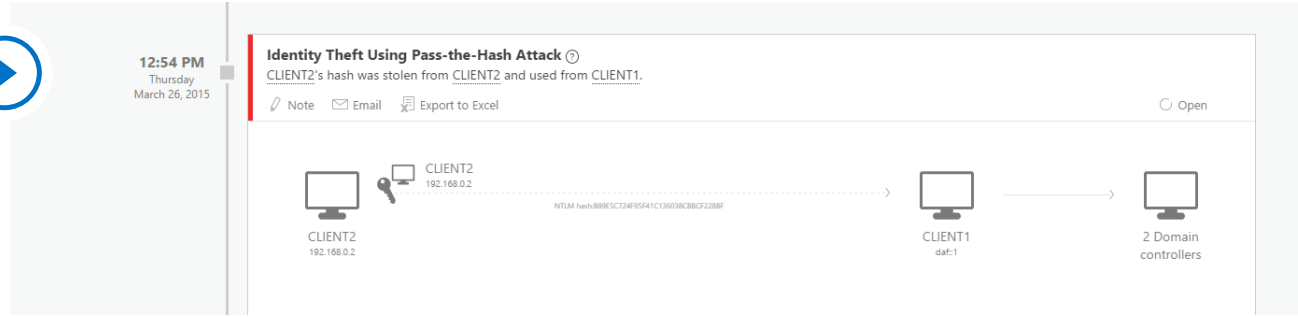
Security issues and risks

- Broken trust
- Weak protocols
- Known protocol vulnerabilities



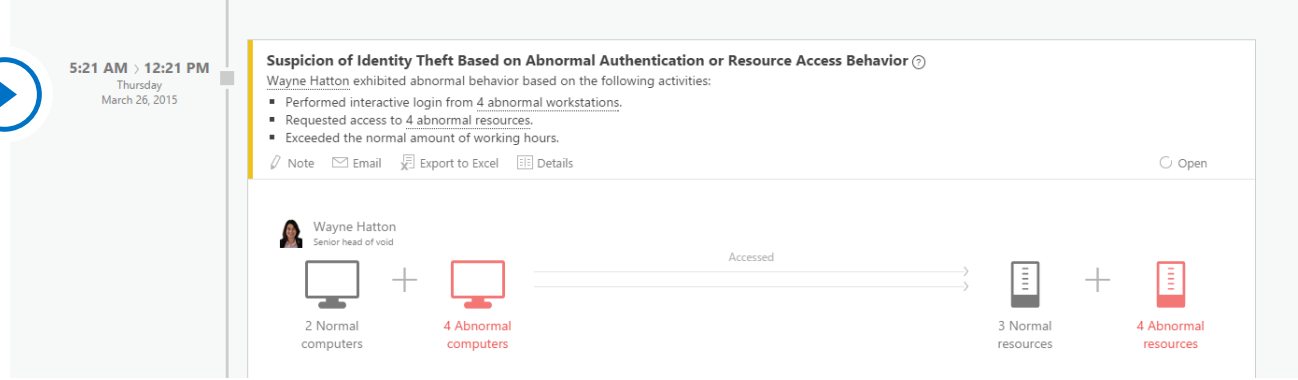
Malicious attacks

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- Reconnaissance
- BruteForce

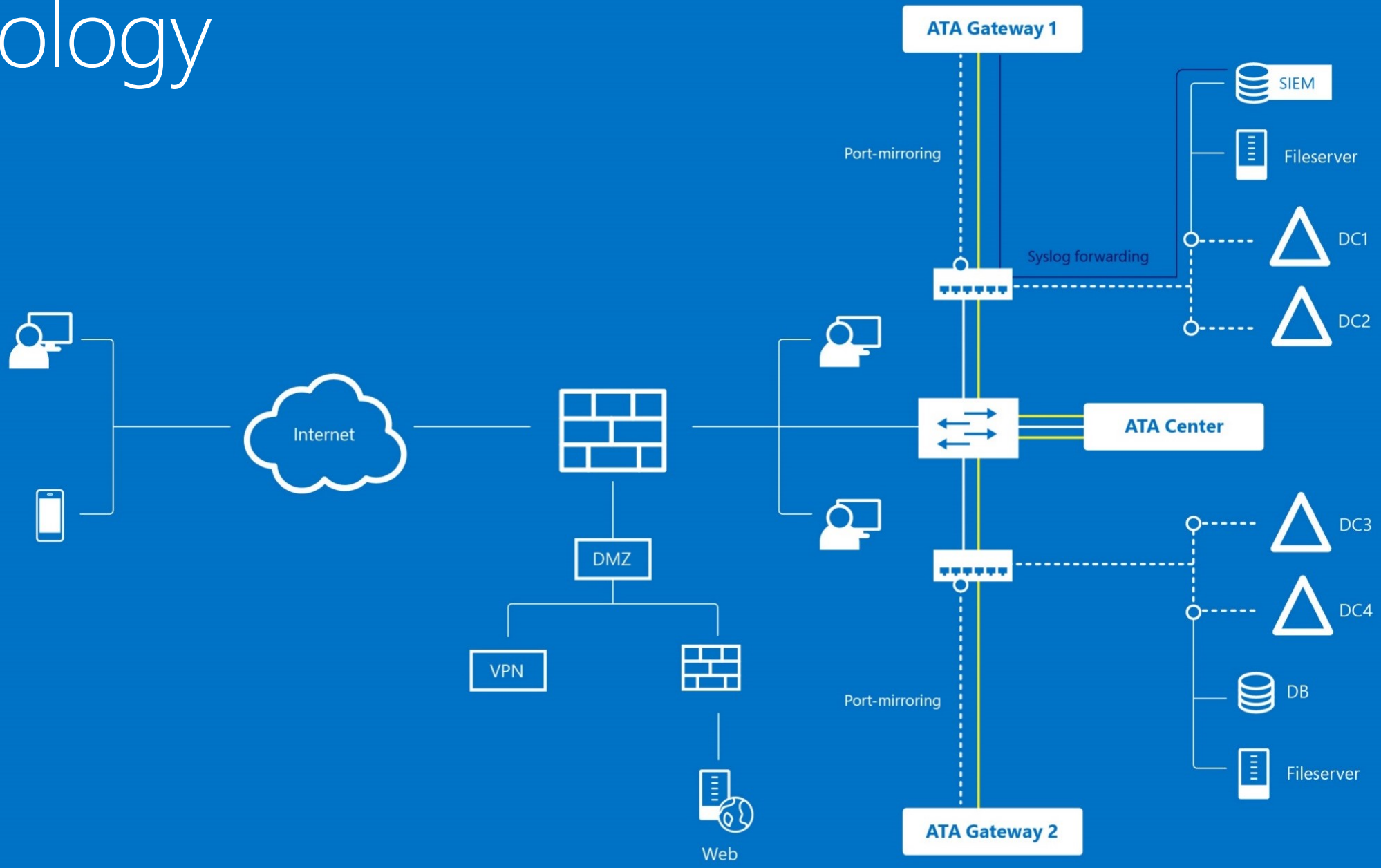


Abnormal Behavior

- Anomalous logins
- Remote execution
- Suspicious activity
- Unknown threats
- Password sharing
- Lateral movement

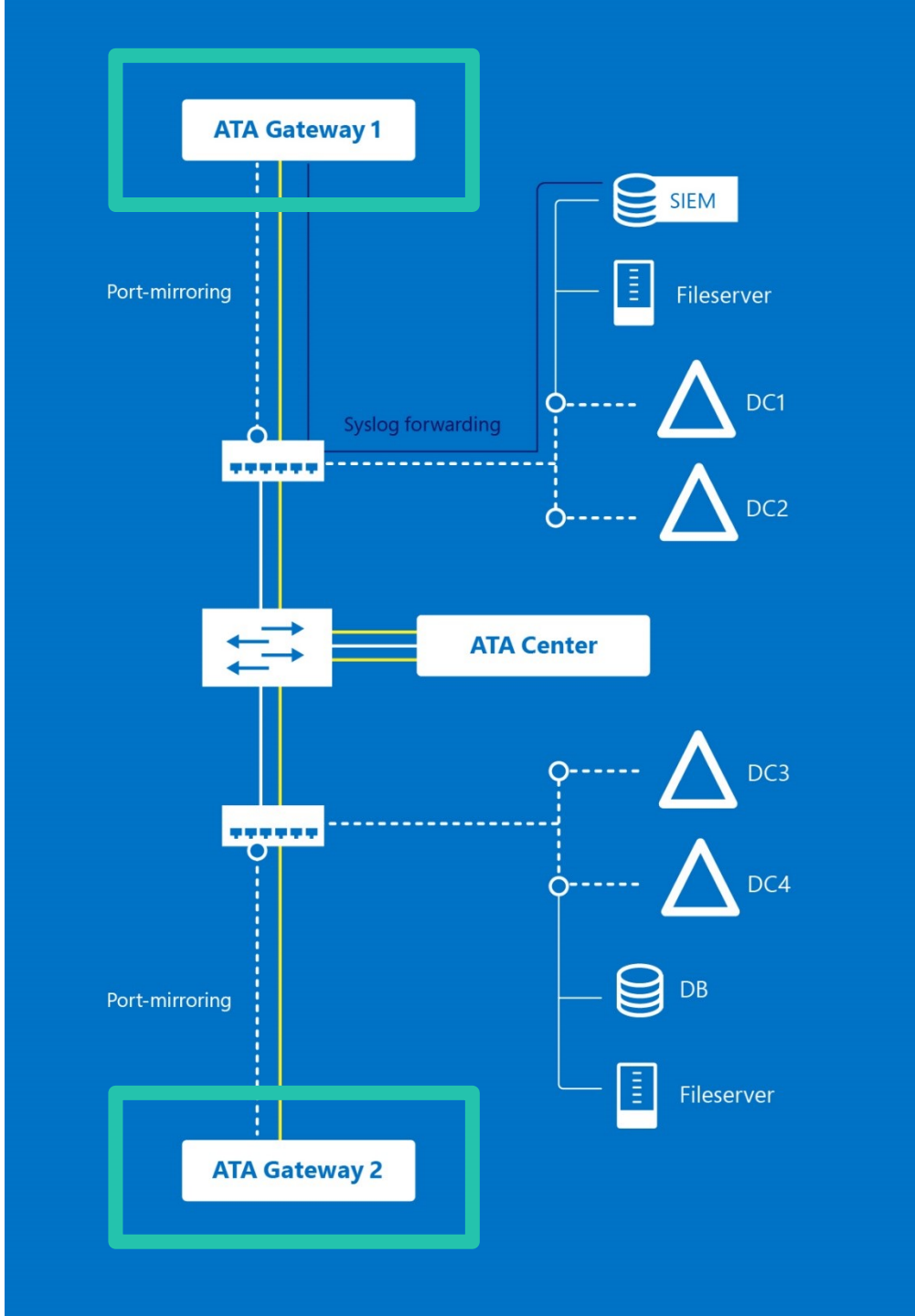


Topology


ATA Gateway 1
SIEM
Fileserver
Port-mirroring
DC1
Syslog forwarding
DC2
Internet
ATA Center
DMZ
DC3
DC4
VPN
DB
Port-mirroring
Fileserver
Web
ATA Gateway 2

Topology - Gateway

- Captures and analyzes DC network traffic via port mirroring
- Listens to multiple DCs from a single Gateway
- Receives events from SIEM
- Retrieves data about entities from the domain
- Performs resolution of network entities
- Transfers relevant data to the ATA Center



Resources

- Advanced Threat Analytics - https://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/
- EMS beyond BYOD - https://mva.microsoft.com/en-US/training-courses/enterprise-mobility-suite-beyond-bring-your-own-device-15707
- Microsoft Advanced Threat Analytics - https://www.youtube.com/watch?v=V57I-EAvdL4
- ATA Prerequisites - https://technet.microsoft.com/en-US/library/dn707709.aspx
- Microsoft ATA Technet Library - https://technet.microsoft.com/en-us/library/dn707706.aspx
- 90 day ATA evaluation version - https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics

CIAOPS Resources

- Blog – http://blog.ciaops.com
- Free SharePoint Training via email – http://bit.ly/gs-spo
- Free Office 365, Azure Administration newsletter – http://bit.ly/o365-tech
- Free Office 365, Azure video tutorials – http://www.youtube.com/directorciaops
- Free documents, presentations, eBooks – http://docs.com/ciaops
- Office 365, Azure, Cloud podcast – http://ciaops.podbean.com
- Office 365, Azure online training courses – http://www.ciaopsacademy.com
- Office 365, Azure eBooks – http://www.ciaops.com/publications

Twitter
@directorcia

Facebook
https://www.facebook.com/ciaops

Email
director@ciaops.com

Skype for Business
admin@ciaops365.com