Concurrency
Digital Transformation Realized™

Concurrency Assists Global Software Solution Provider with Advanced Threat Analytics (ATA) Configuration and Deployment

Background

This global software solution provider serves clients around the world with enterprise resource planning and other software solutions.

To enhance security of the company's internal networks, the client's internal IT team embarked on a project to deploy Microsoft Advanced Threat Analytics (ATA).

ATA Advanced Threat Analytics (ATA) is an on-premises platform that helps protect an organization from multiple types of advanced targeted cyber attacks and insider threats. ATA does so by receiving and analyzing event logs as well as capturing and parsing network traffic of multiple protocols.

The system employs machine learning to identify normal and abnormal network behavior. When abnormal behavior occurs—a potential threat—the activity is flagged and presented to users in a console. In this way, an IT team can avoid the "false positive fatigue" commonly associated with conscientious security monitoring and analysis.

ATA also allows vastly more in-depth review than is possible by even a large team of human technicians.

Solution

Our primary role in this project was to help the client's North America's internal team ensure smooth configuration and deployment.

The internal team is highly experienced. During a short, focused planning workshop we collectively identified requirements and planned the deployment.

One of the most critical aspects of standing up an ATA platform is sizing. Because ATA servers receive and analyze all packets hitting the enterprise's domain controllers, the ATA servers are placed under a heavy computational load on an ongoing basis. Without proper sizing, the addition of the ATA platform can lead to a network bottleneck situation.

After the planning workshop, we initiated a script to help determine that proper sizing.

The next day, we assisted the client's internal team with the actual ATA server deployment in connection to the domain controllers and with their configuration.

We reviewed the dashboard console with the client team through a process that included initiating some non-threat abnormal behavior to demonstrate the ATA system's activity.

Results and Next Steps

This project involved deployment of the ATA solution on a subset of the client's network. Having proven out the concept and successfully implemented the solution on this subset, the client's IT team is now well-prepared for additional deployments across their environment.

With the ATA solution in place, the team—and organization as a whole—benefit from enhanced security through a truly modern approach that:

- Detects threats fast with behavioral analytics;
- Adapts quickly;
- Zeros in on the right alerts; and
- And reduces false positive fatigue.