Azure Advanced Threat Protection

100 XP

5 minutes

Azure Advanced Threat Protection (Azure ATP) is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

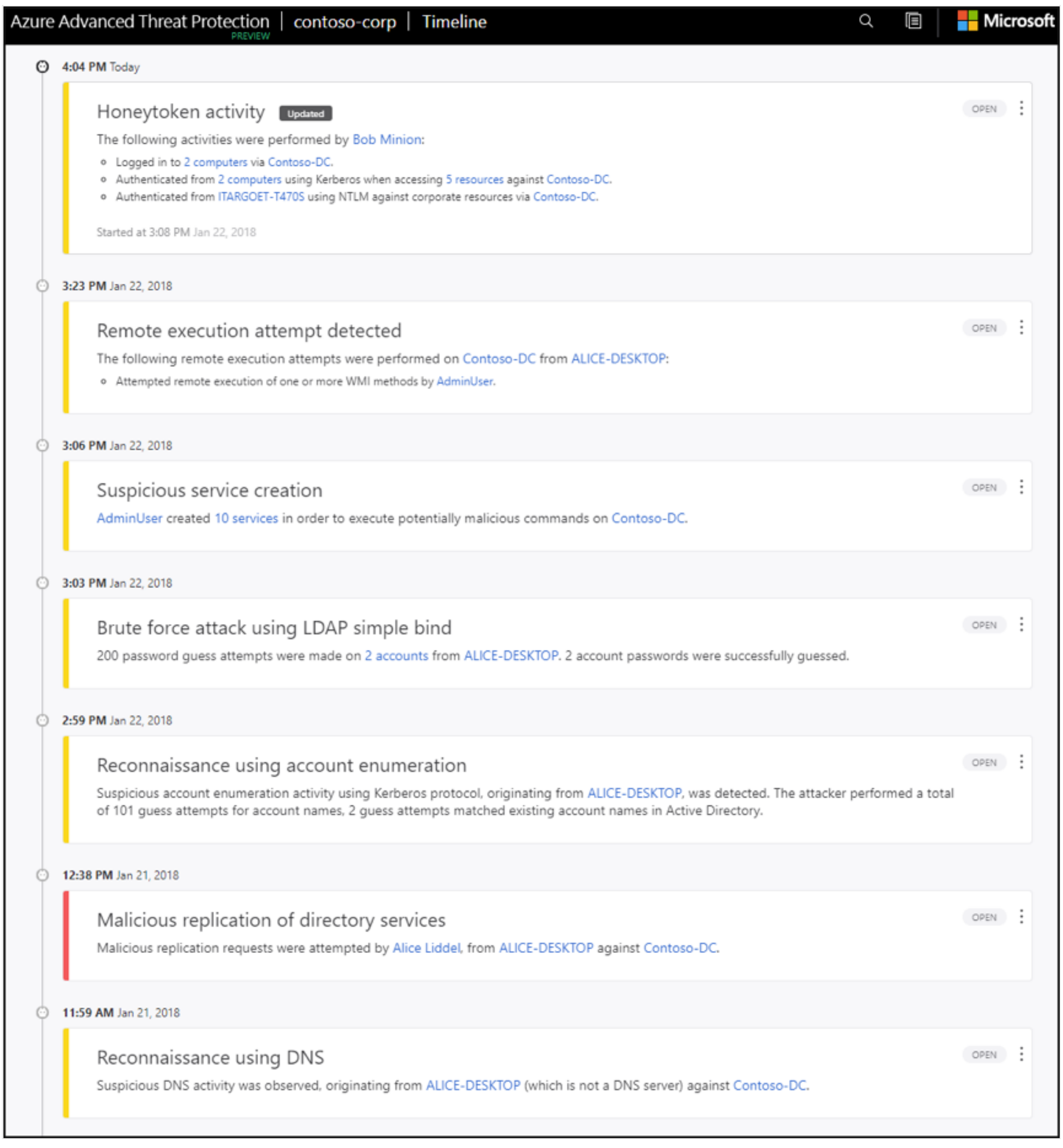
Azure ATP is capable of detecting known malicious attacks and techniques, security issues, and risks against your network.

Azure ATP components

Azure ATP consists of several components.

Azure ATP portal

Azure ATP has its own portal, through which you can monitor and respond to suspicious activity. The Azure ATP portal allows you to create your Azure ATP instance, and view the data received from Azure ATP sensors. You can also use the portal to monitor, manage, and investigate threats in your network environment. You can sign in to the Azure ATP portal at https://portal.atp.azure.com. Your user accounts must be assigned to an Azure AD security group that has access to the Azure ATP portal to be able to sign in.



Azure ATP sensor

Azure ATP sensors are installed directly on your domain controllers. The sensor monitors domain controller traffic without requiring a dedicated server or configuring port mirroring.

Azure ATP cloud service

Azure ATP cloud service runs on Azure infrastructure and is currently deployed in the United States, Europe, and Asia. Azure ATP cloud service is connected to Microsoft's intelligent security graph.

Purchasing Azure Advanced Threat Protection

Azure ATP is available as part of the Enterprise Mobility + Security E5 suite (EMS E5) and as a standalone license. You can acquire a license directly from the Enterprise Mobility + Security Pricing Options page or through the Cloud Solution Provider (CSP) licensing model. It is not available to purchase via the Azure portal.

Next unit: Understand Security Considerations for Application Lifecycle Management Solutions

Continue