PROACTIVE
PART OF / FELLOWMIND

Azure Sentinel
Proof of Concept

Create a functional overview of threats and security incidents

Businesses today are experiencing a vast amount of security threats. Many spend too much time combining and identifying abnormalities and possible incidents in their IT environment. Therefore, numerous businesses have a noticeable need for a solution that supports the organization in focusing on the most important threats. Hereby eliminating unnecessary abstractions when working with IT security.

The user friendly and cloud based SIEM solution: Azure Sentinel, provides an intelligent overview of the most important security warnings and incidents. This enables you and your business to instead spend time where it creates the utmost security value.

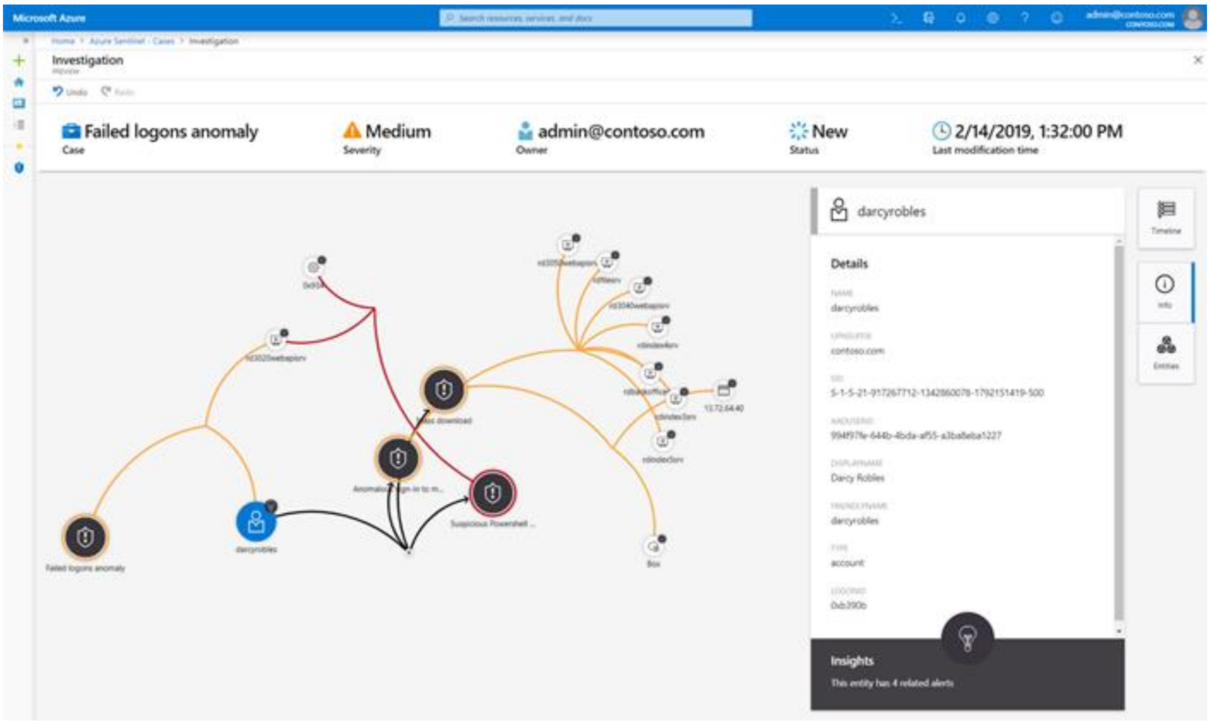
Azure Sentinel uses artificial intelligence to analyze a large number of threats every day, and furthermore filters the noise from the numerous activities. Thus, the service gives you a much better and more focused overview of the threats you should be aware of and be able to react to. Azure Sentinel makes it easy to collect security data across logs from all your devices, including network, firewall, servers, IT systems, endpoints, and cloud. This is regardless of whether they are to be found in your on-premises environment, in Azure, or in other cloud service.

Benefits with Azure Sentinel

- The ability to detect and respond to threats smarter and faster by using Azure Sentinel’s artificial intelligence.
- The minimizing of response time and thereby important time during regular operation or during critical safety-related incidents.
- The creation of a central and focused near real time display of active threats.
- The ability to detect patterns and changes from the norm as well as irregularities in your IT environment.
- The ability to collect data from all sources across your entire business.
- The opportunity to support your company’s use cases and categorize these according to MITER ATT&CK.
- The automation of response to threats. Either with the help of established best practices or by tailored response requirements.
- The ability to easily maintain compliance requirements, e.g., in relation to the GDPR by using historical reports that document compliance.
- Automatic scalability that ensures that your specific needs are met.

PROACTIVE
PART OF / FELLOWMIND

Azure Sentinel
Proof of Concept



Microsoft Azure

Home > Azure Sentinel - Cases > Investigation

Investigation

Failed logons anomaly
Case

Medium
Severity

admin@contoso.com
Owner

New
Status

2/14/2019, 1:32:00 PM
Last modification time

darcyrobles

Details

NAME
darcyrobles

UPNSUFFIX
contoso.com

SID
S-1-5-21-917267712-1342860078-1792151419-500

AADUSERID
994f97fe-644b-4bda-af55-a3ba8eba1227

DISPLAYNAME
Darcy Robles

FRIENDLYNAME
darcyrobles

TYPE
account

LOGONID
0xb390b

Insights
This entity has 4 related alerts

Proof of Concept

If you are interested in taking the first step towards gaining the advantage of Azure Sentinel's many benefits, then ProActive can help you get started with our Proof of Concept (PoC). Our Azure Sentinel PoC unfolds during two workshop days and is composed based on ProActive security baselines.

The purpose of our Azure Sentinel PoC is to give you a concrete understanding of what Azure Sentinel can provide of value to your business. An introduction to how Azure Sentinel can strengthen your security profile based on your environment is presented to ensure that you gain a near real life Azure Sentinel experience.

During the two workshop days we will create an overview of your current infrastructure and data center platform as well as which requirements and needs your baseline meets today. During the workshops, your relevant data sources will be connected to Azure Sentinel. Standard Work Books and Analytics are set up in Azure Sentinel, so monitoring, visualizing and analyzing of your data becomes possible. This ensures a functional overview of alerts and incidents already during the workshop.

Azure Sentinel
Proof of Concept

After the two workshop days, we prepare a PoC report which ensures that you have concrete documentation for your following work with Azure Sentinel. This report contains our safety recommendations to you, and a roadmap, with specific work packages, that describe your possible future implementation of Azure Sentinel.

With ProActive's Azure Sentinel PoC you will obtain:

- A thorough understanding of the possibilities Azure Sentinel contains.
- An analysis of your current security setup (including both your infrastructure and your data center).
- A temporary setup and configuration of your Azure Sentinel solution.
- The first step on the road towards launching Azure Sentinel.