bornінthecloud

Azure Sentinel

Hunt and stop threats before they cause harm, with **SIEM reinvented** for a modern world. Azure Sentinel is your birds-eye view across the enterprise. Put the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI).

Cloud based SIEM?

Azure Sentinel is a cloud-native security information and event manager (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise – fast.

SharePoint/Exchange

SharePoint and Exchange logs have an out of the box connector, allow you to connect to multiple orgs, and its FREE!

Sentinel POC ?

We have a ton of custom IP to help you see value from Sentinel fast. We can also help get past some of the blockers that might be holding you back now.

1. Custom connectors to enrich the out of the box connectors.
2. Hunting queries to help you hunt attackers.
3. Logic Apps to parse logs into a readable fashion
4. Logic apps to remediate attacks
5. Power BI reports to visualise attacks and your hunting tactics
6. ML models for O365

We can help monitor AAD

AAD logs are pulled in with an out of the box connector.

Cisco/F5/Palo Alto

We can connect to a ton of your network appliances out of the box, and we can take all other logs from our custom connectors.

1 Custom Connectors

Sentinel is a single tenant Azure solution. We can pull logs from any Azure or O365 environment. We can also get logs like Intune, WD-ATP and query the Graph API to enrich your data.

2 Hunting Queries

Security alerts need a behavior to be identified, and the facts are that lots of attacks do not raise alerts. But they do leave behavior indications that we can "hunt" for. Hunting often involves multiple data sources, and some ML capabilities built into the Kusto language.

3 Logic Apps to parse logs into a readable fashion

- When you intake logs from Syslog you get a "log inside a log"
- We can run a logic app that will read the "extended properties" and reparse them.
- We keep the original log file so that you can still use that format if you need it for ML models

4 Automated remediation

Enforce MFA, call WD-ATP tasks, block someone from O365, remove a public IP address. All these remediations can happen automatically, semi-automatically, or run manually by a security analysist

5 Power BI reporting

We have a series of Power BI reports that will help you visualise your data and shine a light into some security issues that you have previously found hard to find.

6 Machine Learning – where we start to fight back

With Jupyter Notebooks we can use deep neural network analysis to find behavioural anomalies that do not raise a security alert.

We have developed a ML model that looks at O365 anomalies and with this we can help find the signal from the noise.

Build a better security platform.

We understand O365 logs, the Graph API and the Intelligent Security Graph, at a depth that most others can only talk about.

At the end of this deployment you will have a Sentinel POC that will give you real insights into your security estate.

Want to learn more or get more details? Great! Scan the code and you can email us.

C-Level

www.borninthecloud.com