Data#3

Microsoft Azure Sentinel SIEM

Gold Microsoft Partner | Azure Expert MSP

A recent **study** found that it takes companies up to **206 days to discover a breach**. The average cost of a breach is **$8.7 million**. Can you afford to recover from a breach?

In 2019, **64%** of **notifications** received by the Notifiable Data Breach body OAIC **were the result of a malicious or criminal attack**, with a **19% increase in the number of reported breaches.**

Are you struggling with:

- Collecting signals at scale – across all devices, users and applications, whether it in the cloud or on-premises
- False Positives – Minimise false positives using analytics and Microsoft threat intelligence. The quicker threats are identified, the faster response can be enacted
- Investigation Time – Hunt threats using AI and detect suspicious activity
- Automated Response – respond to incidents using in-built orchestration and automation for common tasks

You need Azure Sentinel SIEM!

What are you missing?

We have found that:

- Customers struggle with the volume of alerts, and have too many false-positives
- Customers have four security consoles on average
- Customers assume Microsoft is responsible for their Azure security

How many consoles do your team have to manage and monitor?

How long can you be offline?

We have found that customers:

- Do not assess the severity of a business continuity threat
- Do not realise that many organisations don't recover from serious breach
- Do not adequately value their digital assets

How do you sequence the remediation activities?

Are you wasting money?

We have found that:

- Customers find security operations more difficult today than 2 years ago
- 70% of customers find it hard to recruit skilled security staff
- Many customers have a proliferation of tools that confuse and add no value

Is it hard to operate your security operations?

What is the Azure Sentinel SIEM Services?

Azure Sentinel is a new SIEM solution that incorporates artificial intelligence and automated response to respond to threats. It can take a wide range of signals from on-premises and cloud solutions. Azure Sentinel can take inputs from M365 E3 or E5, extending this investment into a single, integrated console.

Adopting cloud requires an integrated on-premises and cloud security posture management and view. The Azure Sentinel SIEM service can assist in helping customers to protect their cloud and on-premises estate through the use of an SIEM solution that can take an array of inputs across users, devices, applications and infrastructure. Azure Sentinel can also reduce the instance of false positives by up to 90% and employs automated response for incident response.

"For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control"

Microsoft
Shared Responsibility in the Cloud, 2019

Data#3

Microsoft Azure Sentinel SIEM

Gold Microsoft Partner | Azure Expert MSP

Azure Sentinel secures your organisation

It's a Jungle out There

- Mistakes made in configuration can expose your organisation to compromise
- This can breach compliance with regulatory requirements like. PCI, NDB and GDPR
- Wasted investment in multiple tools that make you less secure

You Need to know What's Going On

- Across cloud, on-premises, applications, servers, virtual machines and end-points
- Reduce console proliferation
- Use automated response to try to shut down attacks as they occur

Leverage our Skills

- Attracting and retaining cloud security skills is difficult
- Leverage Data#3's skills to deploy your SIEM solution
- Protect your organisation from breach before it occurs

What to expect from an Azure Sentinel Service

The Azure Sentinel service will deploy a SIEM solution leveraging the scale of cloud services, and the ability to leverage artificial intelligence to respond to threats. The service will:

- Create a log analytics workspace
- Monitor Azure AD authentication across your user population
- Monitor Office 365 activity (requires E3 or greater)
- Configure 10 core analytics data sources, including tuning

Why Data#3?

Data#3 has the deep expertise your business needs to maximise its investment in Azure. As Microsoft's largest Australian partner, Data#3 has unparalleled competencies in Azure, licensing, system integration and managed services. Our five-stage pathway to cloud success is based on Azure best practices. Whether you are new to Azure or looking for advanced Azure services to take your business to the next level, Data#3 can connect you with the resources and expertise you need.

Your Next Steps

- For more information, visit our **Azure cloud** page.
- Take action today and connect with your **Data#3 Azure experts today**

Interested in how Data#3 can help?

phone 1300 23 28 23
website www.data3.com.au
facebook.com/data3limited
twitter.com/data3limited
linkedin.com/company/data3
youtube.com/user/data3limited