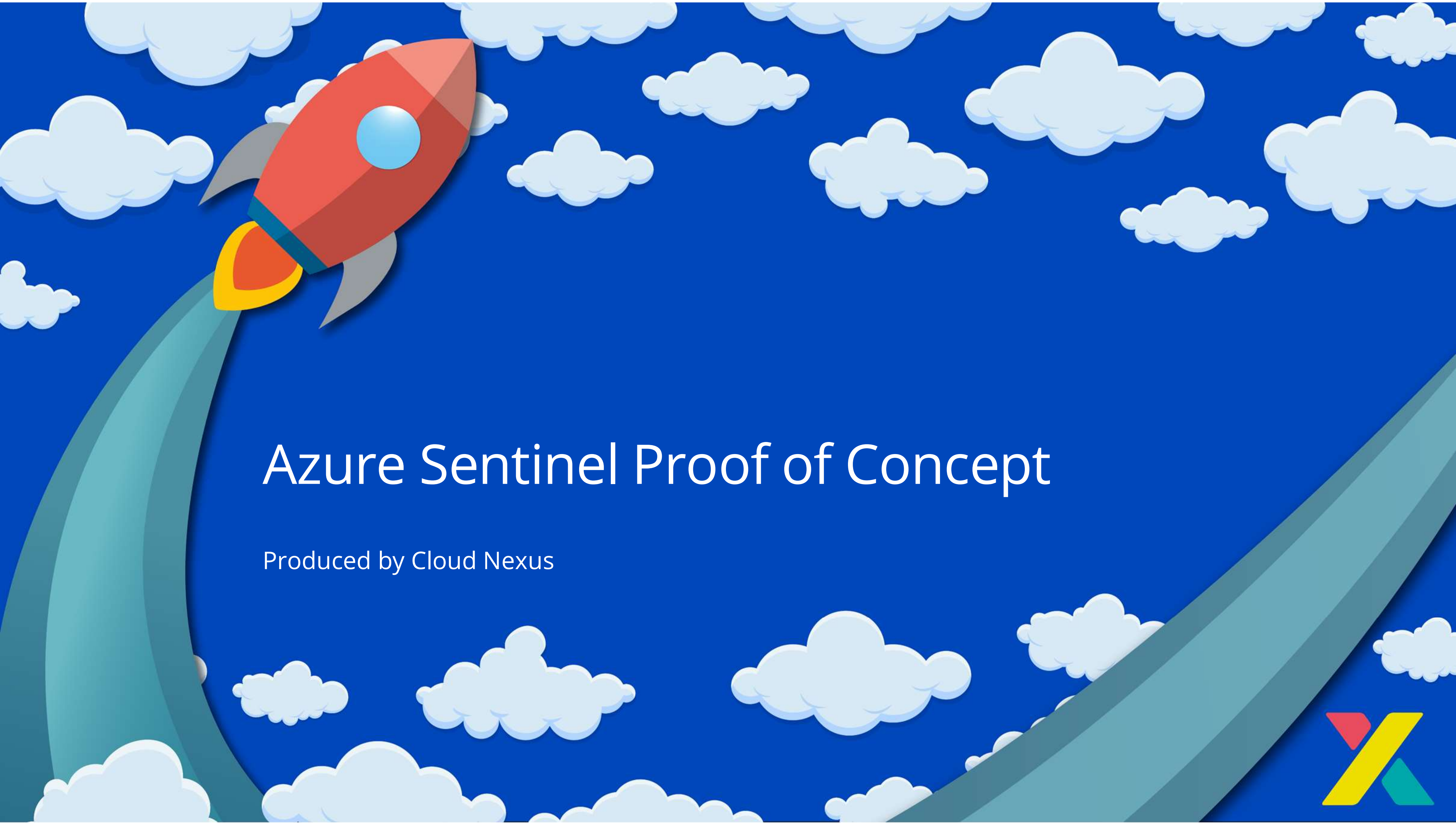

Azure Sentinel Proof of Concept

Produced by Cloud Nexus

Azure Sentinel

Highlights

- Understand the features and benefits of Azure Sentinel
- Gain visibility into threats across email, identity, and data
- Better understand, prioritize, and mitigate potential threat vectors
- Create a defined deployment roadmap based on your environment and goals
- Develop joint plans and next steps

As IT becomes more strategic, the importance of security grows daily. Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges—let alone tomorrow's unimagined risks.

That's why Microsoft developed Azure Sentinel, a fully cloud-native SIEM.

See and stop threats before they cause harm with Azure Sentinel

Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Get an overview of Azure Sentinel along with insights on active threats to your Microsoft 365 cloud and on-premises environments.

> “With everything running through Azure Sentinel, we've reduced the time spent on case management and resolution of alerts by approximately 50 percent”
>
> -Stuart Gregg, Cyber Security Operations Lead, ASOS

cloud nexus

Azure Sentinel

Choose the approach that's best for you

Every business is different, so this proof of concept can be tailored to fit your environment and goals. We can provide either of two scenarios:

Remote monitoring

If your business doesn't have its own Security Operations Center (SOC) or if you want to offload some monitoring tasks, we will demonstrate how Cloud Nexus can perform remote monitoring and threat hunting for you.

Joint threat exploration

If your organization is interested in learning how to integrate Azure Sentinel in your existing SOC by replacing or augmenting an existing SIEM. We will work with your SecOps team and provide additional readiness to bring them up to speed.

What we'll do

Analyze your requirements and priorities for a SIEM deployment

Define scope & deploy Azure Sentinel in your production environment

Proactive threat hunting to discover attack indicators

Discover threats and demonstrate how to automate responses

Recommend next steps on how to proceed with a production implementation of Azure Sentinel

cloud nexus

Azure Sentinel Proof of Concept

Azure Sentinel provides continuous security monitoring of Microsoft 365 behaviour and threats across all users, devices and the core service platforms such as Exchange, Sharepoint and Microsoft Teams. Our service provides a proven deployment model with ready-to-go reports and alerts.

Create a new Azure Sentinel Workspace
Ready to receive alerts from Microsoft 365 data sources

Deploy Connectors for key Microsoft 365 applications
Capture the key information from Azure AD, Exchange Online, Sharepoint, OneDrive and Threat Intelligence

Deploy Monitoring, Reporting and Alerting profiles
This analyses the data sources and applies machine learning algorithms to highlight real threats and provides guidance

Outcomes

Automatically monitor all threat aspects across Microsoft 365. Continuously monitor and improve your security posture.

Machine learning analyses and filters the noise, you only ever get actionable insights

Azure Sentinel protects your business through pre-breach analysis and post-breach investigation

Consolidate security reporting from other platforms into Sentinel for a single source of security risks.

cloud nexus