Need a better way to secure your data?

WE'VE GOT YOUR BACK.

Introducing Azure Sentinel with **LAB³** – a SaaS based SIEM with around the clock support.

Security solutions can come with a heavy price tag and highly specialised systems.

Get better performance and resilience from your cybersecurity with LAB³'s SaaS based Azure Sentinel solution. Our cost-effective solution provides 24/7 monitoring, management and continuous optimisation of your Azure Sentinel investment.

Azure Sentinel is powered by automation – giving you peace mind, so you can focus on your core business needs.

LAB³ is a trusted Gold Certified Security Partner

Starting Right

Fast and accurate deployments by code with prebuilt Playbooks, Alerts and Custom Log Sources templates.

Proactive Response

Harness the ability to respond real time when a security event occurs. Resolving cyberattacks faster with less damage.

Cost Optimisation

LAB³ uses a cost optimization vs. security benefit methodology to ensure our client get the most value out of Azure Sentinel.

Global Security Alliance

LAB³ is the only Australian technology provider to become a member of an exclusive Microsoft partner led security alliance – spanning North America, South Africa and across APJ. The best and brightest in the cybersecurity space join forces to provide the latest Azure Sentinel capabilities to our clients.

What does LAB³ do differently?

Sentinel Setup

We don't just enable Sentinel – we configure and arm it with our extensive catalogue of IP, designed to protect your business in an automated fashion.

Alerts and Playbooks

With hundreds of alert scenarios in our database, we can tailor and target events that are relevant to your business.

SOAR Integrations

Sentinel's SOAR can integrate with an external systems API, to automatically raise and assign incidents based off alerts detected.

Incident Response

LAB³'s cybersecurity team can monitor and action alerts or serve as an escalation point during a cyberattack or post-mortem.

Consultancy & Governance

We can provide expert assistance to tune, enhance and better secure your business using Sentinel - greenfields or brownfields.

Did you know that with an E3 License O365 threat protection using Sentinel is free?

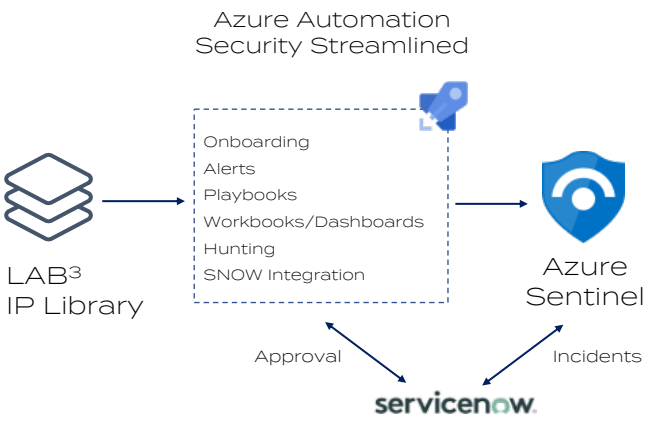
Speak with our team to find out how we can help you start protecting your O365 user base today.

Azure Sentinel
M365, Azure and Custom

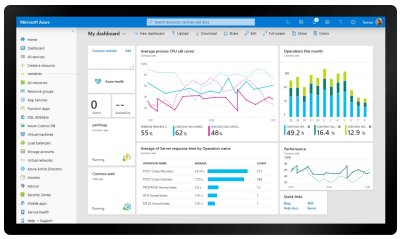
LAB³'s Azure Sentinel solution provides end-to-end cybersecurity capabilities – from setup, onboarding, incident response, governance, to ongoing tunning and cost optimisation.

Our goal is to implement cybersecurity measures that are continually enriched and tuned using Sentinel's own native AI and ML capabilities, combined with LAB³'s real-world experience and automation expertise.

MODERN THREAT PROTECTION
COMBINING AI AND INDUSTRY EXPERTISE



Azure Sentinel
Security Visualised



Our Security Approach

1 DEPLOYMENT
- Azure Sentinel setup
- Onboarding log Sources
- Usage reports
- Threat intelligence Feed
- Silent log monitoring

2 ANALYSIS
- Gather additional requirements
- Review Azure consumption per log source type
- Security value vs. cost assessment
- Present insight report

3 OPTIMIZATION
- Deploy Sentinel alert rules based on LAB³'s Alert Catalogue
- Configure standard playbooks
- Create custom log parsers
- Add additional log sources

4 TUNE-UP
- Sentinel alert rule tune-up match client specific requirements
- Creation of custom playbooks (e.g. ServiceNow)
- Regular meetings with customer security team

Service Elements

SIEM Capabilities delivered from the Azure Cloud	No additional software or hardware to deploy	Support for on-premises log sources (>30 log parsers available)	Security Monitoring of Cloud services (Azure, AWS, Google)	Access to Managed Sentinel Alert Rules Service Catalogue	Performance and availability monitoring and notification	Online access to Alert Knowledge Base
Compliance aware monitoring	Continuous alerts and playbooks tuning and optimization	Support during security incidents	SOAR support and integration	Cloud costs alerting & reporting	Threat intelligence service integration	Monthly service review

*Azure Sentinel SIEM runs in client's Azure subscription *Service is priced based on the number and type of log sources

Get In touch to see if this solutions is right for your business.
hello@lab3.com.au