Need 24x7 Security Detection and Response?

WE'VE GOT YOUR BACK.

LAB³ Security Operations Center

Incident Detection and Response (MDR) + Microsoft Security Services

With dependence on technology increasing, the requirement for comprehensive/total visibility on your security posture is more important than ever.

Knowing you have active and passive defence working together providing insight and intelligent automated protection, reduces your threat vector exposure and increases your governance and security intelligence.

Member of
Microsoft Intelligent Security Association
Microsoft

Homogenous Security

Integration of Security tools to work as a single platform reducing exposure and gaps. Optimising active and passive defence configurations.

Proactive Response

Located in Australia and New Zealand, around the clock coverage, eyes on glass. Protecting your environment responding to incidents and hunting for anomalous activity.

Data Enrichment

LAB³ Threat Intelligence provides attribution with over 400K live Indicator of Compromise (IOC) added daily to enrich the data and provide important insight.

"I am pleased to have LAB³ join us as a partner in the Microsoft Intelligent Security Association (MISA). By including our strategy Managed Security Services Providers (MSSPs) in MISA, we help enable further collaboration between cybersecurity industry leaders in protecting and supporting our joint customers."

- Mandana Javaheri, Director of Business Strategy, Microsoft Security Partner Development

What does LAB³ do differently?

Data Locality

Australia / New Zealand owned and operated.

Data remains in your organisation's tenancy. You remain in control.

Platform Lifecycle

Platform tuning for operational and cost efficiencies.

Platform health reporting showing availability and integration status.

MDR

Active and Passive Defence management.

Threat Detection
Threat Foresight
Threat Response
Threat Hunting

Powered by Automation

Continual tuning of automation for both lifecycle management and incident response.

Leverage LAB3's SOAR IP library.

ISM Compliant

Extend compliance requirements above the Microsoft standard aligning to Information Security Manual by Australian Signals Directorate.

Did you know on average we identify critical security incidents within 12 hours?

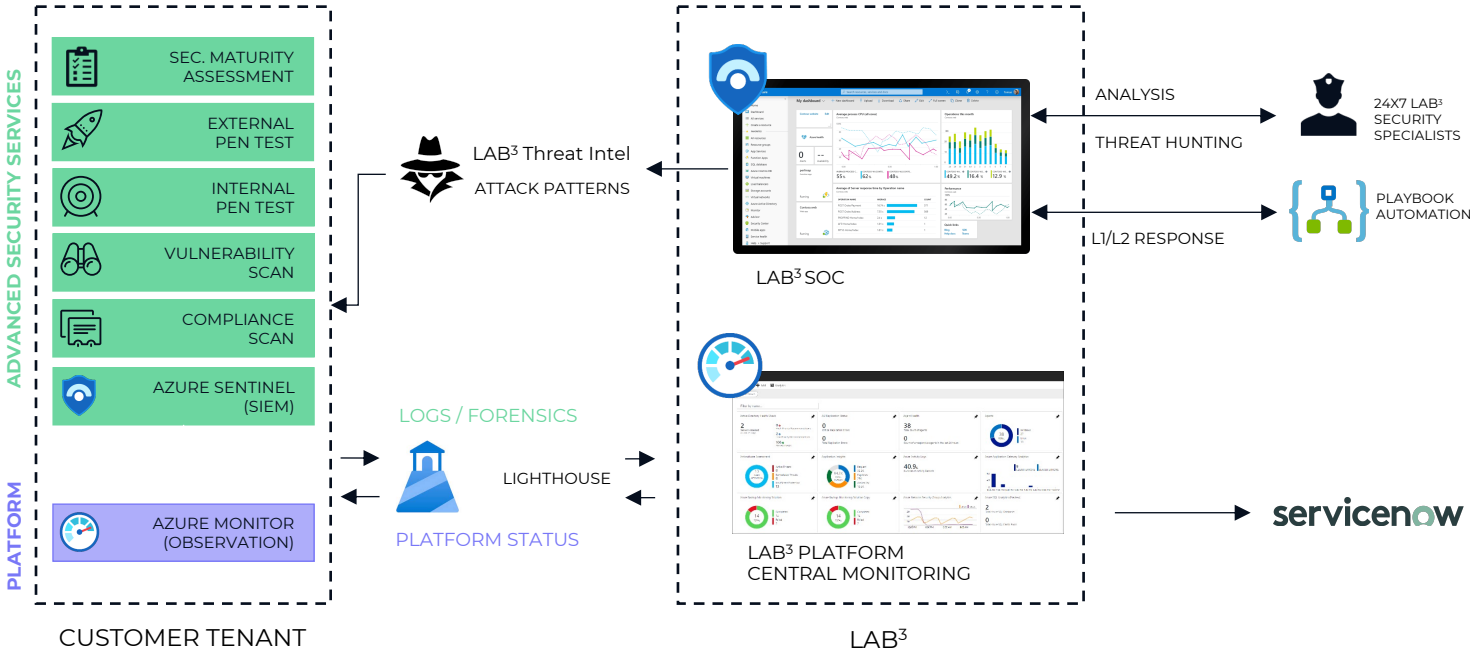
Speak with our team to find out how we can provide a free Organisational OSINT Report today.

LAB³ Security Operations Center

Cloud, Workplace, Hybrid

MODERN THREAT PROTECTION

COMBINING AI AND INDUSTRY EXPERTISE



Our Security Approach

1 AUDIT

Discovery of Client's environment and **Re-affirm** attack vector weaknesses in the people, process and technology.

2 PLATFORM

Uplift to a **Defence in Depth** Architecture. Deploying multiple layers of security controls providing redundancy and protection.

3 UPLIFT

Onboarding and fine tuning of **Active and Passive Defence** security services

4 VISIBILITY

Consolidation of security data providing **Intelligence** into security posture and providing User and Entity Behavior Analytics

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	24x7 Incident Detection and Response	Powered by Automation leveraging SOAR library	Cloud costs alerting & reporting	Incident Attribution with 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