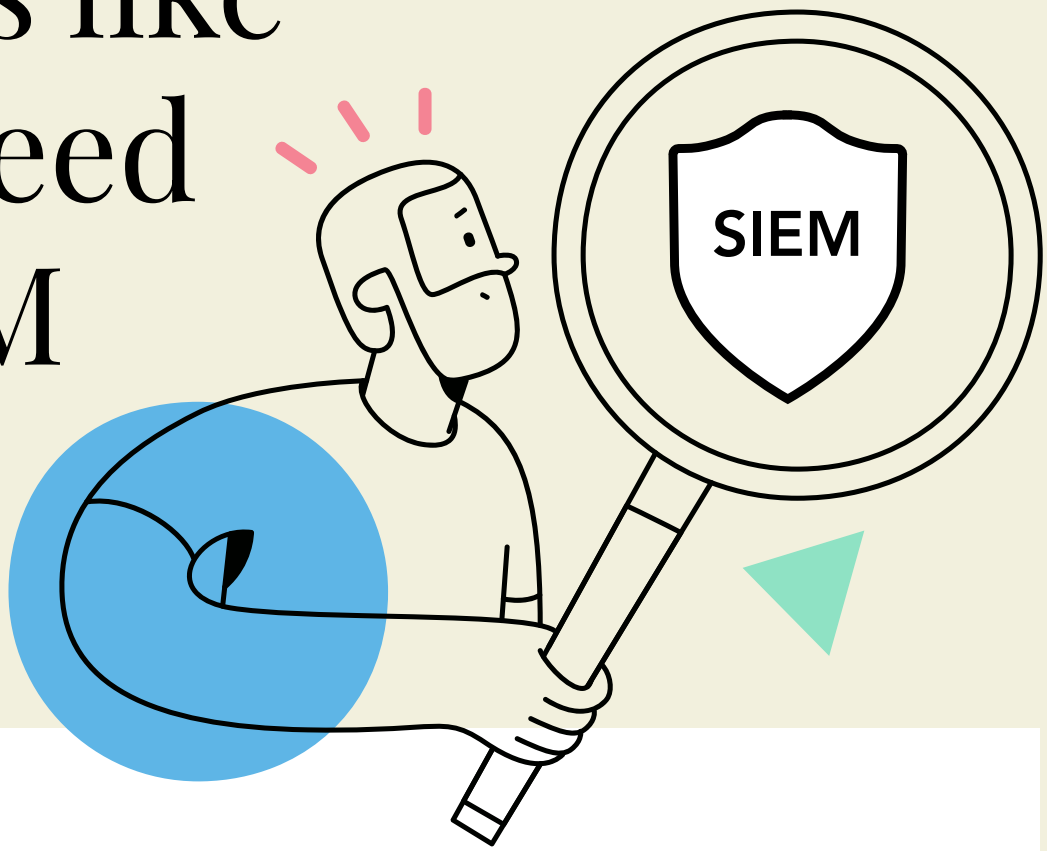
azured

AAT
Australian Amalgamated Terminals

Client case study

Australian Amalgamated Terminals

Seems like you need a SIEM



At a glance

What we did:

- Successful deployment of the market leading SIEM, Microsoft Sentinel, with our Sentinel Starter Kit
- Enhanced incident response through our Managed Sentinel service

Client benefits:

- Centralised security platform that aggregates security logs from all supported and licensed sources
- Visibility is enhanced, with a single dashboard monitoring their security posture
- Management time is saved through our security incidents triage
- Actionable insights mean an appropriate level of response for each alert is provided
- Better value from MS365 subscription and more control over Azure spend utilising our custom-built reporting
- Clear framework for a cloud security roadmap and continuous improvement

All about AAT

Australian Amalgamated Terminals (AAT) is Australia's leading mixed cargo terminal operator, providing an extensive range of terminal services and equipment to facilitate integrated logistics solutions in all the major ports across the Australian Eastern seaboard.

The Challenge

AAT's facilities and services play a critical role in the efficient operation of the mixed cargo supply chain.

Effective risk management and sound governance are core pillars of AAT's corporate strategy; with the responsibility of managing cargo inspections, biosecurity hazards, contamination treatment and customs procedures requiring effective risk strategies. Managing cyber security related risks to protect the company against ransomware and other cyber threats requires a broad, multi-layered cyber strategy. A key requirement of this strategy is clear visibility of their real-time security posture. To that end, AAT required a SIEM solution to consolidate the extensive threat data.

Enter Azured...

What is SIEM?

According to Gartner, "Security Information and Event Management technology supports threat detection, compliance and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources."

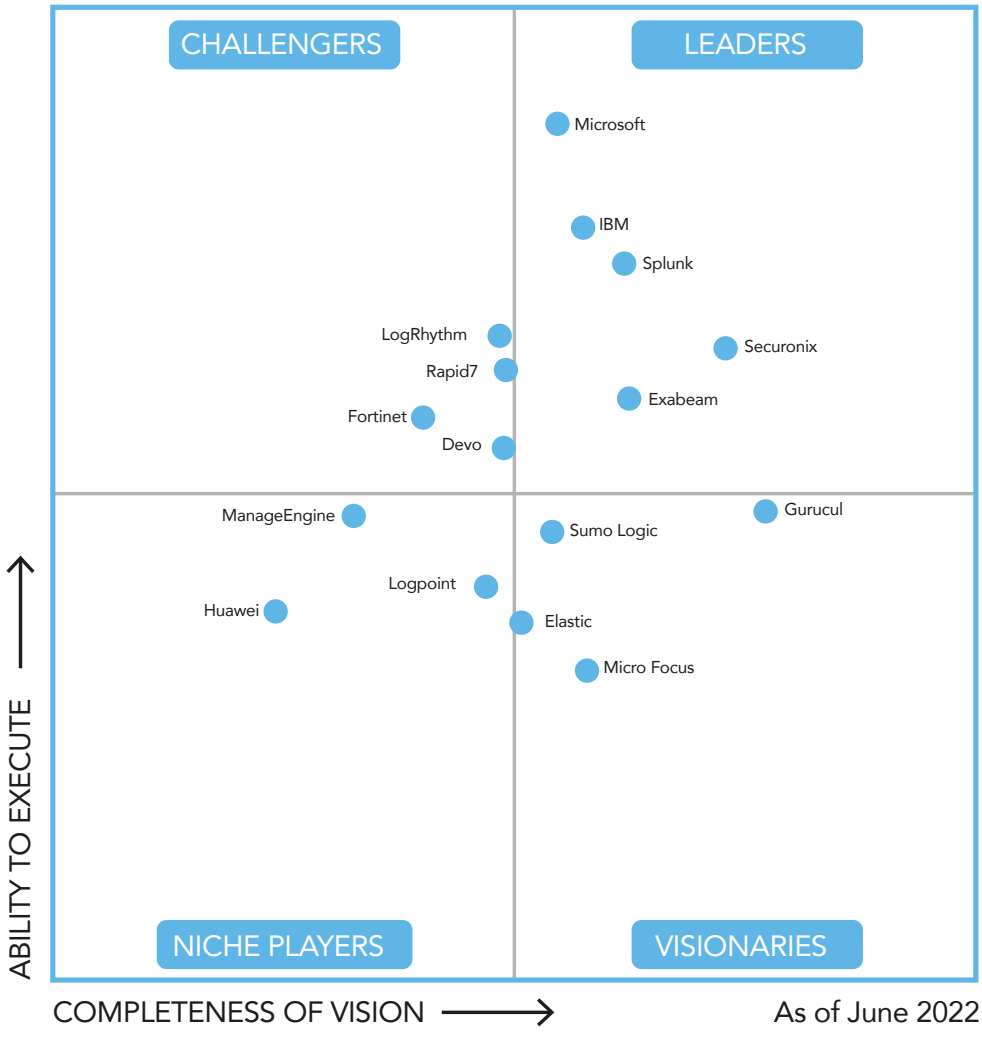
azured

The Solution

The Azured team in Australia, who specialise in all things Microsoft Azure and M365, already had a fantastic working relationship with AAT – having assisted the business early in their digital transformation journey to transition to Microsoft Cloud from Private Cloud. Once it became clear that their valued client was seeking fit for purpose SIEM solution, they introduced our Cloud Security Specialist team, based in the UK.

Working in collaboration with our Australian colleagues and drawing upon their extensive knowledge of AAT's environment, we kick-started the project by undertaking Azured's Sentinel Starter Kit. This project would lay the foundations for the successful deployment of Microsoft Sentinel – the market leading SIEM solution.

Microsoft Sentinel is the leading choice for SIEM



2022 Gartner® Magic Quadrant™ for Security Information and Event Management (SIEM)

azured

Sentinel
Starter Kit

The secret to successful Sentinel deployment

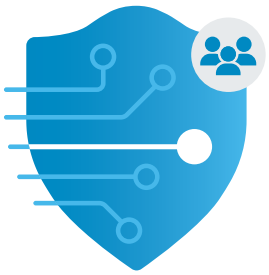
Now, deploying Sentinel is not quite as simple as flicking a switch, not if you want it to do the job as effectively, efficiently, and easily as possible.

Our security sages activated and set-up Sentinel in AAT's environment, by creating their workspace and setting up the data connectors to start feeding the information into Sentinel.

AAT uses an extensive range of Microsoft and third-party security tools, which they were looking for a more streamline streamlined management approach. So, we integrated these into Sentinel's centralised security management portal.

After testing the integrity of the data inputs, we then configured the rules sets that examine the data and makes sense of it. These rules needed to correspond to the types of services that AAT use, and the common attack vectors related to those services.

Our next step was to create customised dashboards that interpret the raw data from Sentinel, showing the information specifically relevant to AAT. We tailored the alerting and reporting functions to notify and display treats logically – filtering through the noise of the alerts and prioritising threats that require a response.



Managed
Sentinel

The fully managed, seamless SIEM

OK. So Sentinel was set-up and running to the best of its (really quite magical) ability. And for some clients, that may have been perfectly adequate. However, AAT spotted an opportunity to further reduce administrative overhead and complexity by engaging Azured for their Managed Sentinel service (which we playfully refer to as SMaaS, because it sounds a bit like a Moomin).

Managed Sentinel takes the responsibility of monitoring threats in Sentinel and response escalation out of AAT's hands and places it firmly in the hands of our security specialists. It's a flat, monthly fee so AAT has complete predictability over their costs.

Our team monitor all incidents and triage high severity incidents – deciding on the appropriate response within the agreed SLA. We investigate the incident and follow the alert trail and based on our knowledge of the environment and the severity of the incident decide whether it needs to be escalated or closed. If advanced investigation is required, then the incident is escalated and handed to Azured's relevant specialist team to deal with the threat.

By creating 'watchlists', a directory of VIP users, applications, and devices, which can be priority alerted through Sentinel if they are exposed to threats, we've customised AAT's security strategy to be in line with what they deem business critical.

Providing this level of dedicated support also allows us to continuously fine-tune and innovate the Sentinel service for AAT, constantly customising the reporting function by filtering and changing variables to present data digestibly, providing visibility of the right information, at the right time.

And wrapped up as part of the service are weekly email reports of notable incidents, ingestion data and costs for running Sentinel as well as comprehensive monthly service reviews. All of which makes for a better night's sleep, for everyone.

azured

Results

Previously, AAT had numerous third-party applications that monitored their cloud security status. By implementing and correctly configuring Sentinel, we created a centralised security platform. Now, not only are all incidents are in one, easy to access place, but are also being analysed by a richer rule set and Microsoft machine learning and AI – giving AAT valuable visibility and control over their security posture.

By moving AAT's security platform to Microsoft, we also helped them get more value for money out of their MS365 subscription, as Sentinel makes use of their existing licensing model, allowing for more services to be integrated. We were also able to give AAT more control over their Azure spend by setting a baseline tailored to AATs specific requirements and creating rules that monitor costs and alert of any deviation.

Our 'incident triage' service means that valuable management time is saved, and effort is expended when and where it needs to be spent, by cutting through the noise of thousands of alerts every day.

By identifying vulnerabilities and escalating them for remediation, AAT now have all the tools and visibility they need to make the right decisions for their business; And as our Managed Sentinel Service includes continuous improvement and innovation, AAT are assured that their cloud security roadmap is fit for purpose, both now and in the future.

"Security is a key pillar of AAT's organisational and ICT Strategy. Our cyber security roadmap is very focussed on risk mitigation and sound governance. As part of that focus, we were looking for specific expertise to enhance our Microsoft Cloud Security profile. Thanks to the knowledge and security enhancements implemented by Azured, we have full confidence in the knowledge that our core business environment is secure."

Vincent Macheda, General Manager
Australian Amalgamated Terminals

If you'd like to know more about how Azured's Sentinel Starter Kit and Managed Sentinel service can improve your cloud security drop our friendly Head of Sales and Technology Partnerships Lead, Elliot a line at elliot@azureduk.com

azured