AARNet Security Operations Centre Services

Protect your campus networks, assets and people from cyber threats

The AARNet sector-wide SOC is a service which is specifically designed to support the security needs of the higher education and research sector by helping institutions to identify, investigate and mitigate security threats.

This SOC service further expands AARNet's portfolio of security services and provides universities with access to real-time security monitoring for their networks, assets, users, and applications.

The service uses machine learning and automation to identify and prioritise security incidents and to help customers with activities such as threat hunting and preventative security measures. SOC customers have direct access to their own data within the AARNet Security Information and Event Management (SIEM) platform to enable optimal collaboration between the universities and the AARNet SOC team.

Our SOC team performs incident triage, investigation and recommends mitigation activities for all identified security incidents. For high severity incidents, the SOC team will advise and support customers throughout the incident response process to ensure threats are mitigated quickly and effectively.

Features and benefits

- ✓ **Real-time monitoring and data analysis**
  Our SIEM proactively monitors your university's traffic and then captures and analyses billions of events 24/7.
- ✓ **Threat correlation**
  The AARNet SIEM uses machine learning and automation to identify and prioritise security incidents and to help with activities such as threat hunting and preventative security measures.
- ✓ **Common platform advantage**
  The AARNet SOC provides the sector with a common platform and tools, enabling playbooks, scripts, actions and other threat intelligence to be shared for the benefit of all participating universities.
- ✓ **Transparent security**
  The AARNet SOC provides customers with access to the suite of SOC tools. This allows customers to run their own search and scripts, develop their own reporting and dashboards, and work collaboratively with the SOC team. This allows for a very collaborative and transparent hybrid SOC approach.
- ✓ **Access to data**
  Universities have direct access to their own data within the AARNet SIEM platform for optimal collaboration between each university IT/Security team and the AARNet SOC team.
- ✓ **Unlimited ingestion of logs**
  The AARNet SOC allows the ingestion of all logs with security and forensic value without limits for the single annual price including data retention for 24 months.
- ✓ **22 university SOC customers**
  There are currently 22 university SOC customers. This provides the AARNet SOC with a wealth of direct Australian threat intelligence and understanding of the Australian higher education sector. Through our on-boarding work with these SOC customers, AARNet has gained substantial experience with log sources and systems that are common across the sector to support threat detection and common playbooks.
- ✓ **SOC scale**
  The AARNet SOC is now ingesting over 12 billion events per day, making it one of the largest SOCs in Australia by data volume.
- ✓ **Incident co-ordination**
  Incidents are investigated, triaged, and escalated to you for threat mitigation. We work with you to develop mitigation strategies and ensure threats are remediated quickly and effectively.
- ✓ **Customised portal**
  View your threat data and collaborate with our SOC team to fine tune your security via a customised workspace in the AARNet SIEM platform.
- ✓ **Fit for purpose**
  AARNet worked in partnership with several universities to design a SOC that meets the unique needs of the research and education sector. AARNet works with university CISOs through a CISO Forum and Cyber Advisory Board (CAB) to continue to improve the SOC services and build the AARNet Cyber roadmap.

- ✓ **Security expertise**
  Our SOC is staffed by a highly skilled team of security analysts and engineers trained to counter cyber threats in the university environment.
- ✓ **SOC assurance through AttackIQ**
  All SOC customers have access to run AttackIQ simulations on a quarterly basis to confirm the SOC's ability to detect defined attacks.
- ✓ **On-boarding support**
  Our dedicated SOC support team understands research and education sector environments and provides all the on-boarding support you need.
- ✓ **Threat intelligence**
  Our SOC integrates with various threat commercial and non-commercial intelligence sources globally across the sector, security community and government to share and receive timely and relevant Indicators of Compromise (IOCs).
- ✓ **SOC-DDOS-ISP**
  As the sector's ISP AARNet is able to integrate threat intelligence that is provided via its SOC and DDOS services directly with its ISP services to protect SOC customers and the sector more generally.
- ✓ **100% sovereign**
  AARNet is 100% owned, operated and hosted in Australia.
- ✓ **Secure infrastructure**
  The AARNet SIEM infrastructure is securely hosted across dual-redundant certified Australian based data centres for improved resilience.
- ✓ **Licensed telecommunications provider**
  As a licensed telecommunications carrier AARNet is held to higher governance standards than unregulated managed security service providers.
- ✓ **Integrated IT Operations Logging service**
  An integrated IT Operations Logging service will also be available to SOC customers in 2023. This will provide a Splunk-like environment with unlimited ingestion and annual FTE-based fees.
- ✓ **Our Partners**
  We partner with a number of commercial software providers for our SOC service including Palo Alto Networks, CrowdStrike, MISP, Exabeam, Elastic, AttackIQ, and SOC Prime, which allows us to bring the best technology the market offers to our overall solution.

Pricing

- One-off on-boarding fee.
- Flat annual SOC fee, based on the number of full-time (FTE) university staff (we don't charge for students). This provides predictable pricing, based on what matters most: protecting an institution's people and their data. Universities are not charged on log volume consumption.

Security Operations Centre Service Offering

Security On-boarding	SOC Workshop	Pre-Engagement Assessment
		Security Operations Introduction and Alignment
	Information Gathering	Asset & User Identification and Prioritisation
		Information Classification
	Data Modeling	API Contextual Integrations
		Network, Asset, User Entity Modeling
Security Monitoring	Real-Time Monitoring	Alert Analysis
		Use Case Tuning
	Behavioural Analysis	User Behavioural Analytics
		Entity Analytics
	Anomaly Detection	Insider Threat
		Fraud
Incident Coordination	Incident Investigation	Focused Monitoring
		vSIRT Support
	Incident Triage	Prioritised Escalation
		Continuous Monitoring
	Mitigation Guidance	Automated Response
		Co-ordinated Incident Response

More information

Find out more about Security Operation Centre Services via AARNet and other services at **aarnet.edu.au** or contact your AARNet Customer Relations representative **CustomerRelations@aarnet.edu.au**

Proudly supported by AustCyber Australian Cyber Security Growth Network

AARNet is an AHECS partner AHECS AUSTRALASIAN HIGHER EDUCATION CYBERSECURITY SERVICE