AARNet Security Operations Centre Services

Protect your campus networks, assets and people from cyber threats

Recent cyber attacks and a number of high-profile incidents have put the Australian research and education sector in the spotlight. Attacks on universities are increasing because of the sensitive data and intellectual property they hold.

The AARNet Security Operations Centre (SOC) is a purpose-built facility that provides Australian universities with the security operations capabilities they need to prevent, detect and respond to cyber incidents and to improve the security posture of the sector.

Features and benefits

- **Real-time monitoring and data analysis**
  Our Security Incident and Event Management System (SIEM) proactively monitors your university's traffic and captures and analyses millions 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 SIEM provides the sector with a common platform, enabling playbooks, scripts, actions and other threat intelligence to be shared for the benefit of all participating universities.
- **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.
- **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.
- **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 intelligence sources globally across the sector, security community and government to share and receive timely and relevant IOCs (Indicators of Compromise).
- **Secure infrastructure**
  The AARNet SIEM infrastructure is securely hosted across dual-redundant certified Australian based Data Centres for improved resilience.

Pricing

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

Security Operations Centre Service Offering		
Security Onboarding	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
		Coordinated 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