IT SECURITY SPECIALISTS

DATA SHEET

Special ALGIM collaborative pricing from $1650* per month + data volume charge *plus GST

Shared Managed Detection and Response Service

Cybersecurity detection and response 24/7 - the power of a team of cybersecurity analysts looking after your council at a fraction of the cost of staffing one analyst

Cybersecurity detection and response

Early detection and response is critical to defending and helping prevent complex cybersecurity risks within your organisation. Unification of the application and cloud logs, with detection of network based events is the only way to identify, classify and defend against complex threats.

Leveraging the best set of integrated technologies, together with our experience in modern incident response, SSS and ALGIM provides an affordable alternative to staffing your own team of cybersecurity analysts.

Using tightly coupled detection and incident response services, subscribers can be notified quickly on potential vulnerabilities or threats within their environment 24/7.

Threat actors never sleep, and neither do we. The use of automation and advanced triage helps remove false positive detection from your environment. Our Cybersecurity Analysts together with our threat response playbooks, help identify potential threats, and provide rapid investigation and remediation advise to you.

Multiple essential security capabilities in one service

Everything you need in managed threat detection and incident response is available for the first time in one service. The elastic scalability of a SaaS solution, combined with insight based reporting to help guide your decisions and highlight areas of potential risk.

Asset discovery

- Network asset discovery.
- Software and service discovery.
- Public cloud asset discovery

Vulnerability assessment

- Network vulnerability scanning.
- Cloud vulnerability scanning.
- Cloud infrastructure assessment.

Intrusion detection

- Network Intrusion Detection (NIDS).
- Cloud intrusion detection.
- Host based intrusion detection.

SIEM and log management

- Event correlation engine.
- Log management with full rention for the life of the subscription.
- Thirty day event and alarm search.
- Retention of logs for the life of your subscription.

Behaviour monitoring

- Asset access logging.
- Cloud access and activity logging (Azure monitor, AWS cloud trail, Cloud watch, S3).
- VMware access logs.
- Microsoft O365 and Active Directory

Key features and highlights

Centralised security monitoring for on-premise and cloud environments

- AWS and Azure public cloud monitoring.
- Windows and Linux endpoints in the cloud or on-premises.
- Virtual compute via VMware of Hyper-V.
- Physical assets in your offices or data centres.
- Cloud applications such as Office 365 or G-Suite.

Incident Response (IR) services

- Automated triage of alarms to reduce false positives and provide context on any indication of compromise.
- Automated response services on detection against critical alarms.
- Access to Cybersecurity Analysts 24/7 for emergency escalation of incidents.
- Five Incident support hours included in service.

Integration with Malware Free Networks (MFN)

- Service provides correlation of events with a near real-time view of the MFN to detect potential threat actors and support remediation activities.

Service management

- Business hours service desk and access to cybersecurity analysts.
- Full platform management and access to service provided automated dashboards.
- Email based service requests for moves adds and changes to service.

Leverage scale

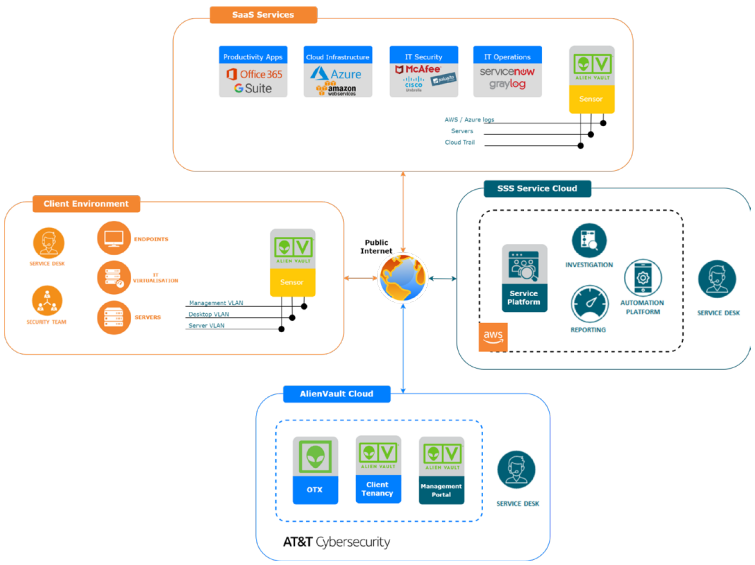
- Group discounts on the platform when purchased together.
- Dedicated reporting for each party.
- Leverage bulk storage discounts.
- Annual discounts available.

Fortnightly reporting

- Written report highlighting the activities and incidents from the previous forthnight.
- Follow-up conference meeting to discuss the findings and recommendations with your team.
- Trend reporting to highlight areas of improvement or focus for next period.
- Platform reporting on data usage and performance.
- Recommendations from threat hunting activities carried out by the service.

Access to threat intelligence

- Service provided Open Threat eXchange (OTX) is available to security teams.
- Detection of possible credential breaches of staff to help mitigate Account Take Over (ATO) activities.
- Detection of potential Personally Identifiable Information (PII) from detection of compromised accounts.



Advanced technology

- Integrated log management and correlation engine.
- Automation and orchestration integration.
- Future automation playbooks available.