SSS Security Operations (SecOps) & Services

IT SECURITY SPECIALISTS

A comprehensive Security Operations solution that you can adapt to fit your budget, desired outcomes and environmental context.

Let us help you stay focussed on the right threats, vulnerabilities and prioritise your efforts.

We have combined our expertise with AlienVault® USM to bring you a powerful Security Operations solution.

Why AlienVault®?

- Asset and software discovery and inventory.
- Security intelligence – constant monitoring, analysis and correlation of user behaviour and logs with automated alerts, based on your priority for security incidents.
- Intrusion and anomaly detection and alerting on network, host, wireless and cloud environments.
- Automatically prioritise identified security events.
- Continuous vulnerability monitoring with authenticated and unauthenticated active scanning options.
- File integrity monitoring to monitor changes to critical files.
- Compliance monitoring for PCI DSS.
- Visibility of dashboards, incident details and log information.
- Over 19 million threat indicators contributed daily.

Benefits of the SSS SecOps service

- Select only the components that you need and define the level of service you want to meet your specific requirements.
- Only pay for the hours / time consumed up to the agreed amount.
- Monthly payments with no minimum commitment (cancel anytime!). Discounts apply on contracts of 12 months or more .
- Free no obligation trial / demo available.

SSS SecOps overview

If you don't have the resources or skillset required to effectively review and action security intel – the SSS SecOps service is specifically designed for you.

SSS can act as an extension to your team to help ensure you are focused on the right threats and vulnerabilities.

Want to know more? Contact us today for a free demo / trial.

SERVICE COMPONENTS

Platform management & support

Including patching and maintenance of the SIEM platform as well as working with your change management process.

Monitoring

Including daily monitoring of the service, alerts, system health and dashboards.

Monthly Actionable Reporting

Customised reporting to suit your requirements.

At a base level this includes:

- Vulnerability statistics (new, closed, older than 90 days)
- Security event summary
- Top hosts by event
- Top users by event
- Top recommendations
- Progress on remedial activities

Remediation prioritisation and coordination

We help you understand your remediation priorities and where to focus your efforts.

Incident management & response

This includes threat hunting, investigation management and reporting.

Forensic Analysis

Including specialist forensic analysis and reporting services.