# Security Information & Event Management ("SIEM")

3Si Security & Event Management provides a consolidated platform to allow organisations the ability to monitor and manage threats and anomaly events on their network. The solution is provided as an 'all in one' virtual appliance which allows customers to easily snap the solution into their existing environments and immediately begin collecting, managing and reporting on the status of the network. The focus is to provide a highly functional solution whilst keeping to the 3Si model of an intuitive user experience.

## Key Solution Benefits

### Discovery - Asset Collection

- ✓ Once the 3SI SIEM device has been added to the network it will immediately begin active network scanning and collection of information on the assets within the environment.
- ✓ In built asset inventory allows you to keep detailed information on discovered assets.

### Vulnerability – Detect & Remediate

- ✓ The 3SI SIEM device will continuously scan the network in search of vulnerabilities.
- ✓ Vulnerabilities will be immediately alerted on the monitoring dashboard and allow engineers to quick isolate and remediate the issue.

### Monitoring – Logs/Netflow & Service Availability

- ✓ Log collection will take effect immediately and data and statistics will be available within around thirty minutes of implementation.
- ✓ Netflow statistics will break out the source, destination and class of network traffic. This data is then graphically reported on to show potential issues with congestion on the network.
- ✓ Availability monitoring via a customisable dashboard shows what is happening right now and where potential breaches and outages may occur.

### Intelligence – Correlate, Alarm, Respond

- ✓ Thousands of standard correlation rules are built in to the product and the customer has the ability to define custom correlation rules as required.
- ✓ In built alarming will alert based on pre or custom defined thresholds with integration options to many common alerting and service desk tools.

| | Standard | Advanced | Premium |
|---|---|---|---|
| Processor | 4 CPU | 8 CPU | 12 CPU |
| Memory | 8GB | 16 GB | 24 GB |
| Storage Usable RAID 5 | 1.8 TB | 2.8 TB | 4.8 TB |
| Estimated Events Per Day (EPD) * | 20 Million | 80 Million | 120 Million |
| Estimated Events Per Second (EPS)** | 220 | 900 | 1250 |

* ** Estimated based on industry standards. Will vary based on customers network environment configuration.

For more information please visit www.3sisecure.com