Managed licence service

Pre-configured packages with five security use cases

As part of the managed licence service, pre-configured cyber security packages starting from 20GB ingestion per day are available from £16,000 + VAT per annum which combine the appropriate professional services to deliver five security use cases and dashboards alongside support and administration training credits.

Use cases - overview

The following 5 searches and use cases/dashboards are implemented as part of this pre-configured cyber security package:

1. Secure your internet connection
2. Secure your users
3. Control access to your data and services
4. Protect your institution from viruses and malware
5. Monitor devices and software

Use cases - details

1. Secure your internet connection

Build a dashboard detailing traffic flowing through the firewall.

Highlighting:

- Unexpected SMTP Traffic
- Unexpected DNS Traffic
- Unexpected SMB Traffic
- Firewall login activity
- Firewall policy change events

2. Secure your users

Build a dashboard detailing account activity.

Highlighting:

- Users not changed password in X number of days
- Inactive user accounts for over 90 days (requires Splunk to be running for +90 days)
- First-time access within the last seven days
3. Control access to your data and services

Build a dashboard monitoring usage of privileged accounts.

Highlighting:

- Active directory account usage with excessive admin privileges
- Identify changes to user accounts that grant this privilege
- Logons using the administrator account
- Track application installation events
- Track new scheduled tasks
- Track new batch job creations
- Track service creation events

4. Protect your institution from viruses and malware

Build a dashboard to monitor malware events.

Highlighting:

- Software versions
- Signature versions
- Failed signature updates
- Malware by criticality, and status
- # Infections over time
- Malware variants over time
- List of systems that have not been cleaned

5. Monitor devices and software

Build a dashboard to monitor updates.

Highlighting:

- Failed updates and reason
- Items found but not installed
- Updates and current status