Skybox Managed Services Description

Date: 2021-01-23

Version: 6.4

Confidentiality: PUBLICLY SHAREABLE

SKYBOX™ SECURITY

FORESIGHT® CYBER

TABLE OF CONTENTS

1 INTRODUCTION

Good vulnerability and configuration management have consistently been critical processes in limiting the exploitation of engineering weaknesses in systems – vulnerabilities, misconfigurations, overly open network firewalls - by cyber threat actors: manipulation and corruption of poorly managed systems being the leading cause of information security incidents.

Skybox Security suite of products allows organisations to:

- Efficiently manage misconfigurations found in network devices
- Perform virtual penetration testing thereby producing Indications of Exposure[1]
- Prioritise remediation of vulnerabilities based on threat intelligence
- Permits the creation of and the mimicking of 'real-life' attacks using what-if scenarios
- Firewall management enhancements:
    - Streamline the change process
    - Improve the quality of changes
    - Boosts firewall assurance

Foresight Cyber, a certified Premier partner of Skybox Security, has considerable experience in Skybox management and maintenance, having built a special relationship with Skybox engineering and support teams. We have successfully designed and built a bespoke set of processes, supported by open-source and internally developed tools that allow us to deliver highly effective and efficient security services to our clients.

Our services deliver:

- Fully functioning, updated and performing Skybox Security platform with all licensed modules
- Accurate results generated by Skybox software ensured by having accurate, up-to-date network, asset and vulnerability data in the Skybox model
- Integration to other client's IT and security systems delivering great ROI
- Reports that are available and distributed to various stakeholders

[1] Indications of Exposure (IoE) reveal potential for specific threat actors to successfully exploit the vulnerabilities in systems

2 SERVICE DESCRIPTIONS

Our Skybox services are structured as follows with the stated objectives:

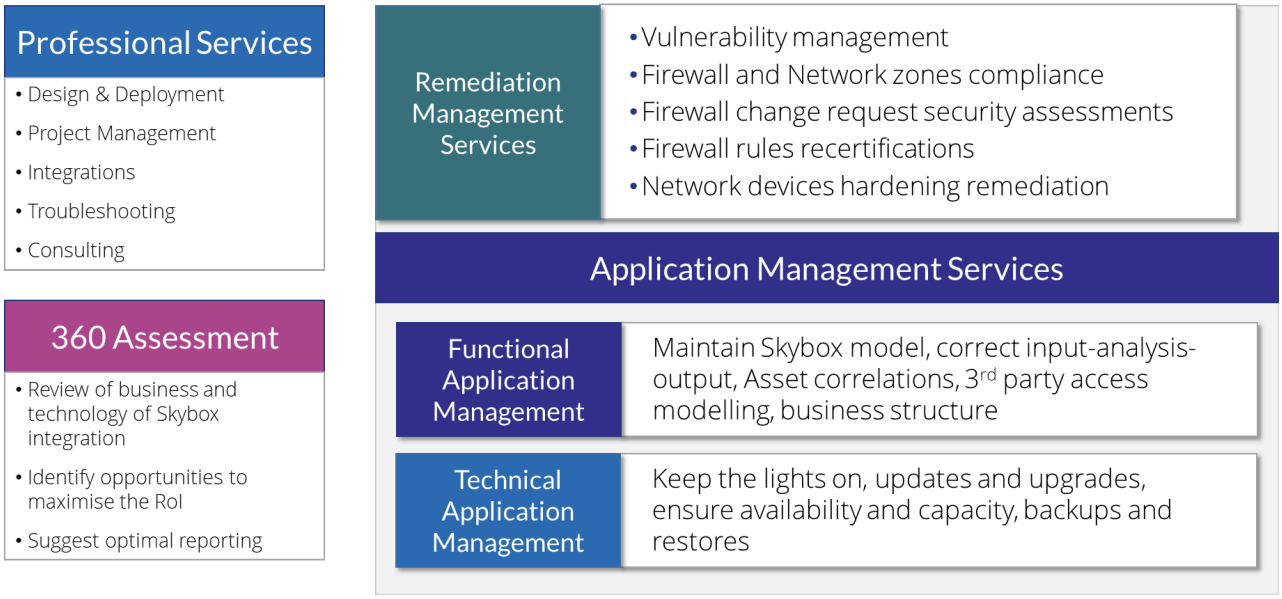

Figure 1 - Skybox Managed Services

This document covers the following services:

Application Management Services

1. Technical Application Management – ensuring the Skybox servers and collectors work optimally, both OS and Skybox application is updated to the latest agreed version, and the application is available to all users

2. Functional Application Management – ensuring the data in Skybox software is up-to-date, correct and available to stakeholders

Remediation Management Services

Orchestrating remediation of issues discovered by Skybox in all licensed modules. Operating Skybox Change Manager for firewall change analysis.

We support any of the Skybox modules a client has licenses for. All services produce relevant reporting available to various stakeholders.

2.1 Skybox Technical Application Management service

The purpose of this service is to keep Skybox server and all collectors operational optimally, with up-to-date software, valid licenses and processes are taking care of any issues related to performance, software bugs, network and user access, and security.

Figure 2 - Skybox Technical Application Management service - high-level components

2.1.1 Operating system management

We fully manage operating system of Skybox server(s) and collector(s). We ensure the operating systems of Skybox servers and collectors are managed correctly and are up to date. Where the operating system is managed by a 3rd party, e.g. Skybox is simply an application on top a client's OS, we monitor the update levels and issue service tickets for the 3rd party to update. The updates are discussed with the client and only processed once agreed.

SLA:

- Weekly monitoring of new versions of operating system patches
- Request to approve an update install within 5 working days and agree an installation window

2.1.2 Availability and capacity management

We monitor all servers using our Foresight Cyber Platform.

We monitor Disk space, CPU usage, memory usage, network capacity and database IOPS for both Skybox servers and collectors, and integration with other key systems (such as DNS, email, Internet access). All abnormalities are reported to the Foresight Cyber Platform's Zabbix monitoring component, issues are investigated and resolved. A customer can get access to the monitoring portal and obtain reports.

Where allowed by customer, we install Zabbix agents on hosts inside the customer network and monitor accessibility of Skybox application from the user's point of view.

The obtained data points are input into capacity management process where we advise customer of any sizing issues and optimisations.

If Skybox is configured in High-availability state (HA), we also monitor its health and recover from HA issues.

We also reconfigure memory and swap configuration to optimise the memory usage.

Note: Zabbix agents must be installed on all Skybox servers and collectors for this service to work.

SLA:

- 24/7 automated monitoring
- Availability and capacity issues assessed within 8 working hours and remediation work done to the best of our ability, and if not possible, issues are escalated to client's IT teams.

2.1.3 Skybox software updates and upgrades

On top of updates to the baseline operating system, our teams monitor for available Skybox application updates and initiate a process of updates upon reaching agreement with a client.

As part of this service, we:

- Keep Skybox server(s) and all collectors up-to-date to minor versions: a schedule is agreed with a client with respect to versions and speed of updates
- Upgrading to new major versions as agreed by a client
- Upgrading the ISO version of Skybox underlying operating system (e.g. Centos 6 to Centos 7)
- Testing updates and upgrades on a test Skybox server (where available)

We inform clients of the availability of updates and upgrades, agree the scheduled installation date and raise necessary changes in client's change management system.

SLA:

- Weekly monitoring of availability of updates.
- When a new version is available for production install, we assess the suitability of the update and create a report to a client within 5 working days and request permission to update.

2.1.4 Licence monitoring and management

Skybox usage is limited by number of licenses for each module. We monitor the number of objects in the model, compared to purchased licenses. When a threshold is reached (typically 80%) we inform a client.

SLA:

- Daily automated monitoring
- On reaching threshold, we create a report to a client within 1 working day.

2.1.5 Backup and restore

We ensure that the Skybox data, scripts and any other files needed for Skybox service are properly back up. As part of the service, we produce a design document, gain approval by the customer, and deploy the backup service. We then test restores annually.

We use progressive incremental backup. Data blocks will be stored to allow the quickest possible restoration. Backups contains daily snapshots of Skybox appliance, all it's collectors, scripts, settings, and historical models.

We agree RTO and RPO with clients, typically 2 working days and 24 hours respectively.

During and after the execution of a backup the Foresight Cyber Monitoring system checks whether execution has been successful.

When a replacement Skybox appliance is delivered (RMA process) we ensure it is properly restored.

SLA:

- Daily automated backups are executed and monitored.
- On client's request or in case of disaster, we initiate restore within 8 working hours.

2.1.6 Skybox User, Roles and Access rights management

Usually, Skybox is setup and configured as part of the project phase, and this includes the right access roles and users. Our service builds on the initial setup and ensures that organisational changes are correctly reflected in the Skybox user access control design.

On request, we create, modify or delete a Skybox user. We also modify the access model to reflect changing requirements.

Key deliverables of this service component are:

- Correct list of allowed users with correct privileges is maintained

SLA:

- On request, a new user is added, old removed, or privileges changes within 2 working days

2.2 Skybox Functional Platform Management Services

The purpose of these services is to keep the Skybox model and data fresh, accurate and reflecting client's network, systems and CMDB.

Please note: Service components are dependent on Skybox modules licensed

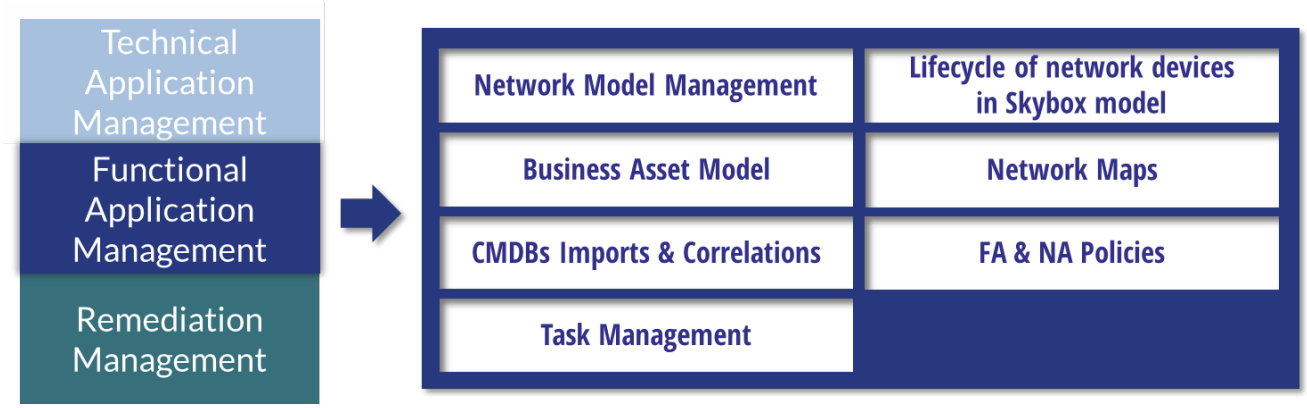

Figure 3 – Functional Application Management service - high-level components

The individual components of this services are explained further below.

1. Skybox network model maintenance

This service component is dependent on either NA or VM licenses which enable network model management.

To enable geo-reporting in the client's reporting portal (or as part of our optional reporting service), we automatically update the *"Site"* attribute of each asset based on its placement in "*Locations & Networks*" or data in CMDB.

When the exact Longitude and Latitude values are known for each "*Site*", we ensure these are copied to all site assets. This allows placing of assets on world maps in the reporting portal.

The key deliverables of this service component are to ensure that:

1. The "*Locations & Networks*" structure is correctly representing the client's current Layer 3 networks
2. The Skybox model is validated, and the validation progress is measurable
3. During our bi-annually reviews of the network architecture, the network teams assert that the Skybox network model exports are accurate.
4. The "*Site*" attribute is populated with a Location name for all assets
5. The geo tags are populated in all assets when exported to CSV

We use Skybox standard model reporting and our Foresight Cyber Platform to perform our analysis. We work closely with a client's network teams and, as such, we establish lines of communications with key stakeholders within each group.

Where we encounter challenges in obtaining sufficiently accurate answers from client's network teams, we escalate this to the client's management.

SLA:

- Model issues analysed on daily basis and analysed within 2 working days
- Where our team cannot autonomously correct the network model, we create incident tickets to client's IT teams
- Automated process requiring client's input of exact location for each site
- The enrichment is setup within 2 working days from the site information receipt

2.2.1 Lifecycle of network devices in the model

We take care of adding new devices and new technologies to Skybox by setting up collections. Similarly, when devices are no longer needed, we remove these for the model and collection tasks. As part of the service we ensure that the model is validated after these changes.

Disclaimer: Foresight Cyber need to be integral part of internal processes for installation and decommissioning of network devices.

Key deliverables of this service component are:

- 100% of client's network devices are collected into Skybox
- Decommissioned network devices are no longer collected and removed from the model

SLA:

- When informed of a new or decommissioned device, our team adds/removes it to collection sequence within 1 working day

2.2.2 Maintenance of Skybox network maps

A visual representation of the Skybox model using network maps presents an advantageous feature. However, the maintenance of individual network maps can be challenging and time-consuming. Our service delivers the up-to-date and well-presented maps for:

- The whole organisation's network
- Each site

Also, we can export these maps to Visio files and save these to the client's designated file system, e.g. SharePoint or a file share

The key deliverables of this service component are to ensure that:

1. The maps are available for users to view
2. Maps are up-to-date with the latest network and asset model changes
3. Visio format maps are saved to a designated file share (as agreed with a client)

SLA:

- Monthly monitoring of maps for any update and export to Visio within 4 working days of the update detected
- New maps created within 4 working days

2.2.3 CMDB imports & correlations

Configuration Management Database (CMDB) is an ITIL term for a collection of databases containing data and metadata about all assets in an organisation. All ITIL processes use the CMDB, and as such, this is a key component in any business.

For Skybox to deliver the business value, it needs network assets to be enriched with CMDB information. As part of this service, we connect up to 2 supported[2] CMDB to Skybox and setup the imports of selected data objects and attributes to the Skybox model.

[2] As part of our service, we support ServiceNow or any other structured data in XML, JSON or CSV format.

The attributes could include, but are not limited to:

- Domain
- Business owner
- Technical owner
- Criticality
- Compliance requirements
- Site
- AWS, Azure Tagging

Where required, we create user custom attributes in the Skybox model.

We monitor the imports to ensure that the data is updated in Skybox as soon as the CMDB data change occurs.

We create an analysis reports that show any mismatches between the Skybox and CMDB(s) asset data. This includes assets that are in one set but missing in others, and where critical attributes may be or are different. Reports are generated in a structured format – CSV or XML. We can also create service tickets for IT teams to fill in gaps in the CMDB. This service generates reports on a weekly basis.

Disclaimer: This service relies heavily on good data quality within both CMDBs and Skybox.

The key deliverables of this service component are to ensure that:

1. Imports are setup and running as per the required schedule
2. Agreed attributes are populated with imported values
3. Detailed reports are generated for client consumption
4. Service tickets are created for IT teams to fix CMDB irregularities
5. Skybox HORIZON reporting structure is maintained to reflect the Skybox model

SLA:

- Daily (or as agreed) CMDB imports to Skybox setup automatically and monitored of issues
- Any importing issues investigated within 2 working days

2.2.4 Business asset model

The purpose and benefits of this service are to group assets in the Skybox model into logical groups, thus allowing different asset viewpoints.

Figure 4 shows our recommended business asset structure. The second level (e.g. Business units, Applications, …) is created as Business Units in the Skybox model. The third level is established as individual "Business Asset Groups" and assigned following attributes:

- Assets that belong to the Business Asset Group – this is done either via a query (e.g. all assets with specific hostname pattern) or by specifying individual assets. We can group assets based on any attribute in the Skybox data model, even user attributes, e.g. AWS tags
- Business Impact – Confidentiality, Integrity and Availability level impact or financial/monetary impact if these assets are compromised. The client provides this information to our team.
- Compliance – any compliance requirements ensuring that these assets are in scope

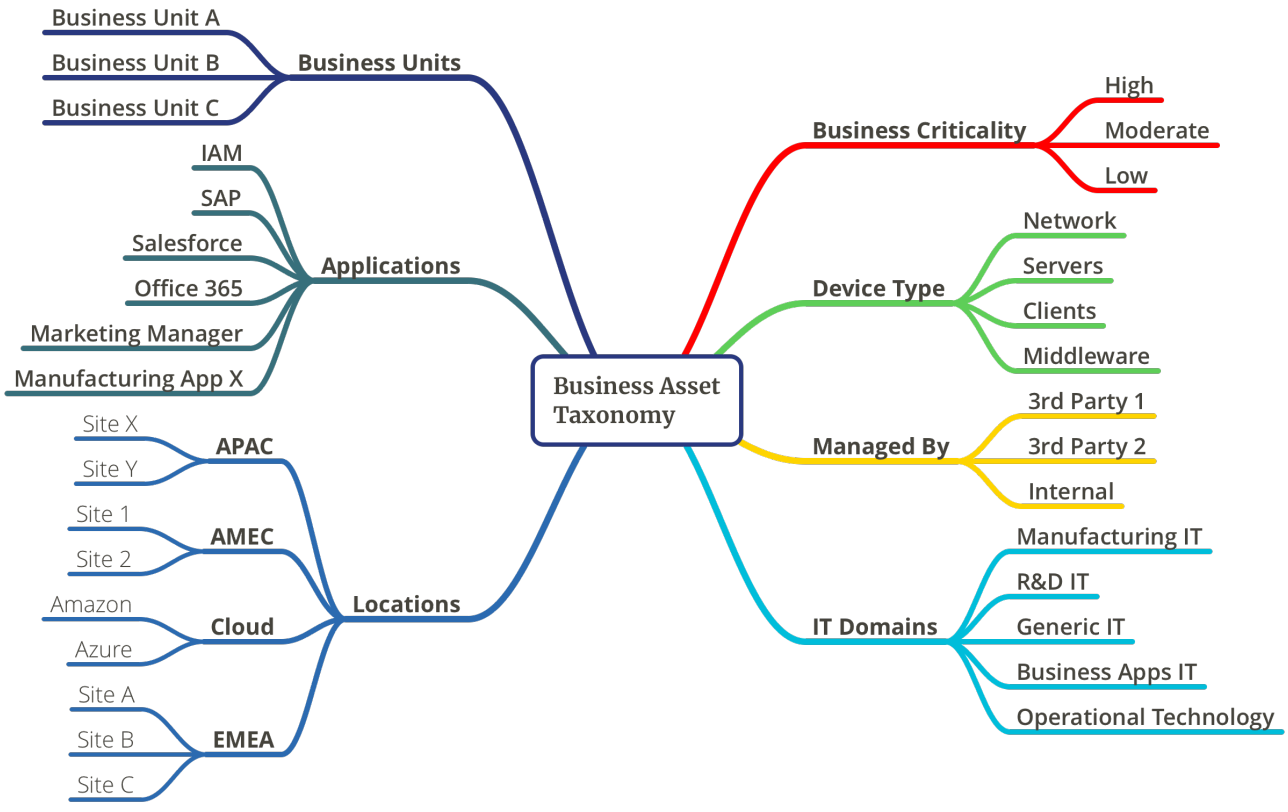

Figure 4 - Business Asset Model example

Key deliverables of this service component are:

- A replica of the "Locations & Networks" structure under "*Business Units & Asset Groups -> Locations*"

- A tree of business applications under '*Business Units & Asset Groups -> Applications*' populated with a list of IP assets that support these applications. The mapping between an application and IP asset(s) is provided by the client
- Other tree structures created as per availability of the metadata in a client's CMDB

SLA:

- As this service component relies mostly on input from a client, we cannot guarantee time-based SLA

2.2.5 Firewall and Network Assurance policies management

This service component is dependent on either NA or FA licenses which network zone and firewall policies.

2.2.5.1 POLICIES

If a client have their own firewall/network policy our professional service team will translate this into a code and add to Skybox. Otherwise, we maintain two firewall and network configuration policies respectively – standard and high-security: these are based on industry best practice. As part of this service, clients can request changes to policies on a quarterly basis, which are then implemented as part of the service.

Skybox supports following policy types:

- Access policy – From-To policy, typically used for zone-to-zone access rules. Access policy requires zones assigned to interfaces on firewalls
- Rules policy – zone agnostic rules related to firewall rules
- Configuration policy – configuration security hardening of firewalls & routers

2.2.5.2 ORGANISING FIREWALL TO FOLDERS

We organise imported firewalls into firewall folders by:

- Service providers, or
- Firewall types

2.2.5.3 NETWORK ZONES

We assign interfaces, networks and tags into correct zones. Such is applicable when clients have licensed the Firewall and the Network assurance modules respectively.

Key deliverables of this service component are:

- A standard and high-security policies are created and approved by the client
- Reports of compliance are generated for client's teams to view on request
- Zones are assigned to interfaces and networks according to information from service providers.

SLA:

- We create and update policies within 5 working days of the receipt of client's policies
- We assign network interfaces, tags, and networks to zones as per client's documentation and instructions within 5 working days

2.2.6 Management of Skybox tasks

To maintain and ensure precise network and asset models, the tasks in the operational console must run accurately and without errors. Our team monitors all tasks, analyses errors and initiates rectification workflows to remedy the issues.

Our team also manages the changes in tasks after the Skybox project finishes initial configuration.

These changes could involve:

- Adding new import and collection tasks
- Changing existing tasks
- Modifying tasks sequences and schedules
- Removing jobs no longer needed

Key deliverables of this service component are:

- All tasks run as per agreed plan without errors
- Changes to tasks are made within the agreed SLA

SLA:

- Issues with tasks are monitored on daily basis and remediation initiated within 1 working day
- For requested changes to tasks and sequences, the work will be initiated within 2 working days

2.3 Remediation Management

Our Managed Services substitute client's Security Operations analysts primarily by delivering remediations for issues discovered through Skybox software.

These service components are available in the MSSP service and can be individually selected.

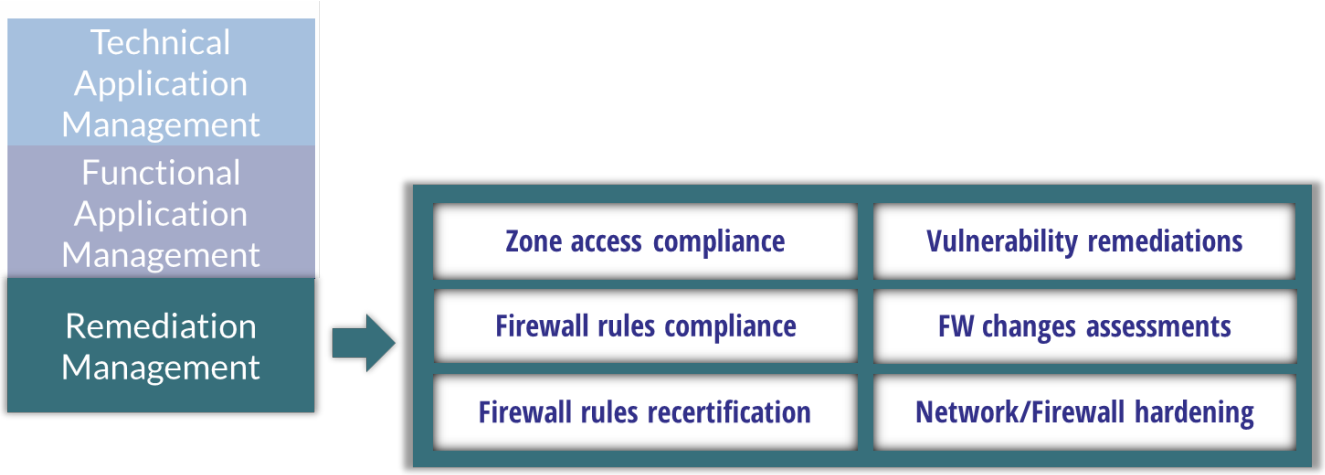

Figure 5 – Remediation Management- high-level components

1. Zone Access Compliance

One of the key values in Skybox is capability to compare the configuration of individual firewalls (requires FA license) or whole network model (requires NA license) against client's zone access policies. This service relies on Application management service 'Firewall and Network Assurance policies management'.

As part of this service, we manage zone access policies in Skybox, on high-level illustrated as a table.

From -> To	Internet	Zone A	Zone B
Internet	No access	Limited access	No access
Zone A	Limited access	---	Full access
Zone B	No access	No access	----

Our teams then monitor violations of these zone policies and raise incident tickets as agreed by customer to remediate.

We also produce monthly reports showing compliance against the policy.

Key deliverables of this service component are:

- Incident tickets for violations
- Policy compliance reports
- Orchestration of fixes through ticketing systems and managing escalations

SLA:

- Daily monitoring of zone policy violations
- Raise incident ticket within 2 working days of the discovery

2.3.1 Firewall rules compliance

This service requires FA licenses. As part of this service we analyse firewall rule bases for compliance irrelevant of zones, taking into account client's firewall policies.

Key deliverables of this service component are:

- Misconfigurations are remediated through raised incident tickets
- Report of remediations

SLA:

- Weekly assessment of rule base compliance compared to a policy and raising incident tickets as per client's policy

2.3.2 Firewall rules recertification

This service relies on Change manager module to be licensed. As part of this service we orchestrate firewalls rules for re-certifications (a functionality in Skybox Change Manager) and manage the workflow. The recertification is a process mandated by firewall management best practices, and essentially reconfirms whether a firewall rule is still valid.

For this service to be correctly delivered, our team needs information about rules that are in firewalls and who should be in the recertification workflow.

Key deliverables of this service component are:

- Firewall rules on all or selected (prioritised) firewalls have gone through regular re-certifications

- A report of recertification process compliance

SLA:

- Rules are added to the recertification workflow within 20 working days before the policy deadline is reached, as defined by client's policy
- Monthly reports generated showing progress of recertifications and overall compliance

2.3.3 Vulnerability remediation orchestration

Skybox provides vulnerability information for collected network devices (via Vulnerability detector and requires FA or NA license) or for collected vulnerabilities for other assets (requires VM licenses).

As part of this service we use client's vulnerability management policy, use Skybox to analyse vulnerabilities, and raise incident tickets to remediate vulnerabilities. We typically try to group remediations based on patches, operating systems or sites; depending on agreement with a client.

For raise incident tickets we ensure the IT teams or providers are processing these towards successful remediations.

Key deliverables of this service component are:

- Vulnerabilities are remediated through raised incident tickets
- Report of remediations

SLA:

- Daily assessment of vulnerabilities compared to a policy and raising incident tickets as per client's policy

2.3.4 FW rules changes assessments

Firewall rule changes present core threat to clients, mainly through non-compliance and risks a firewall ruleset change can represent. Skybox Change Manager provides capability to run any firewall request through a workflow that calculates compliance and risk score.

As part of this service, we are able to analyse firewall requests and return compliance and risk scores. This workflow can be done upfront or ex-post actual firewall ruleset changes.

The actual implementation depends on existing firewall change process that is implemented by a client.

The following diagrams show two workflow options:

Up-front assessment

SLA:

- A firewall request / change is analysed within 8 business hour of the request receipt, provided all required information are available

Post implementation assessment

SLA:

- A firewall request / change is analysed within 2 business days of the firewall change implemented

Key deliverables of this service component are:

- Assessment of firewall changes for risk and compliance
- An escalation raised when an implemented change is outside of risk/compliance parameters
- A monthly report of all changes and their compliance and risk

2.3.5 Network/Firewall hardening

This service requires either FA or NA licenses. As part of this service we analyse hardening of network devices against agreed hardening standards.

Key deliverables of this service component are:

- Misconfigurations are remediated through raised incident tickets
- Report of remediations

SLA:

- Weekly assessment of hardening compliance compared to a policy and raising incident tickets as per client's policy

3 ADDITIONAL INFORMATION

3.1 Service management

Our service includes quarterly service reviews with a dedicated Service manager. These are conducted online using our communication system – Skype for Business, and on request on-site, subject to agreement on travel cost.

3.2 Service delivery and availability

Our services are delivered from SOC offices in the Czech Republic. The team operates 8:00 to 17:00 Europe/Prague local time. We can discuss commercial implications of supporting clients outside of these hours and even 24/7.

3.3 Contacting our support team

Our service is designed to be semi-automated: therefore, it is imperative that communications between the Foresight Cyber support team and the client team are always maintained as tightly as possible.

Our team is accessible by email and Skype for Business – individual engineers, have named accounts, and these are shared with clients at the start of the service.

3.4 Service reporting

As part of our service, we generate service level reports for each service.

Our reporting uses an Elastic Stack, and we encourage clients to request access to our reporting portal for easy dashboard access.

We use the following as part of our service reporting:

- Each service component is reported on its implementation and quality
- Network model issues – current state, over-time progress, geographical view of issues
- Asset management – assets with issues, e.g. missing fields, stale assets
- SLA reports – are the changes and issues resolved within agreed SLAs

3.5 Requirements for the service delivery

To deliver excellent service we require the following:

- A client must have a valid support agreement for Skybox software
- Introduction to key stakeholders with clear communication of the service
- Agreement of way of working with network, firewall, asset management and security teams
- Admin access to the Skybox application
- Admin access to the Skybox server and all collectors
- One or more virtual Foresight Cyber Platform appliances; its technology setup as outlined in Foresight Cyber Platform high-level overview document
- A site-to-site VPN between our Security Operations Centre (SOC) and the client's network; or other means of secure access, as per client's IT standards
- We install Zabbix agents on client's Skybox server and collectors. These interact with our Zabbix server via the Zabbix proxy running on the Foresight Cyber Platform
- The Foresight Cyber Platform needs access to client's DNS, CMDB(s) and an incident management system

3.6 Our Security controls

We are fully committed to protecting the data of our clients and that of our own to the highest standards. We are Cyber Essentials Plus certified.

Our cyber security controls follow internationally accepted standards – NIST Cyber Security Framework and NIST 800-53. Our systems are hardened to industry standards, namely CIS.

We supply details to our clients and partners on demand.

4 APPENDIX A – SPECIFIC T&C

These T&C are taken from our standard service T&C and placed here for situation where different T&C framework is governing a contract.

- The Customer owns the rights to its data as data controller, and Foresight Cyber acts as data processor on the Customer's behalf. All processing by the Company of the personal data and other data provided by the Customer shall be in accordance with the applicable laws. The Foresight Cyber's processing of personal data on behalf of the Customer shall therefore only be done in order to provide the Services and shall be subject to the Customer's written instructions.
- As the Foresight Cyber is data processor and the Customer is data controller, the parties' obligations regarding the processing of personal data are regulated in the data processor agreement attached hereto as the Appendix A. By accepting these Conditions, the Customer also accepts the data processor agreement.
- The Customer is obligated to ensure that the personal data provided by the Customer and used in the Services is processed by the Customer in accordance with all applicable laws. The Customer is obligated to ensure that the Customer's data provided in the Services, including personal data, do not violate any third-party intellectual property rights and/or any applicable legislation. Foresight Cyber is entitled to delete any data that in the sole discretion of the Foresight Cyber constitutes a breach of the aforesaid undertaking by the Customer, and the Customer will not be entitled to any compensation in that respect.
- If the Services are not performed in accordance with this Service Description, Foresight Cyber shall re-perform such Service (or portion thereof). Customer hereby accepts that re-performance shall represent its sole remedy in connection with the performance of the Services.
- All technology, knowledge and processes created prior or during the delivery of the service are intellectual property of Foresight Cyber Ltd.

Foresight Cyber Ltd

Registered & Business address UK
71-75 Shelton Street,
Covent Garden, London, WC2H 9JQ,
United Kingdom

Business address CZ:
Fryštátská 64/9, 733 01 Karvina
Czech Republic

Contacts:
UK Office: +44 20 8159 8942
General enquiries: info@foresightcyber.com
Finance team: finance@foresightcyber.com
Data protection Office: dpo@foresightcyber.com
Directors: directors@foresightcyber.com

https://foresightcyber.com
@foresightcyber.com

VAT: GB144735213
Company number: 06871193
D-U-N-S number: 211601017

OUR CERTIFICATIONS

aws CERTIFIED Solutions Architect Associate

CISSP® ISSAP®

CCSP™

CISSP® ISSMP®

CISSP®

CISCO CERTIFIED CCNA

CCSK™ Certificate of Cloud Security Knowledge

CYBER ESSENTIALS PLUS

Qualys®

SKYBOX™ SECURITY