Description of Services

The following document describes the various services offered by Cyber Defence Corporation (CYDEF), including optional Professional Services.

It also describes the roles and responsibilities for the End Customer and CYDEF with regards to Managed Services.

Managed Services

1. SMART-AV

The service provides monitoring, detection, automatic response, and alerting capabilities to End Customers.

1.1. Basic Protection – Deny list, Signatures and Heuristics

The basic configuration offers protection against known malware and ransomware, such as a Deny list (a database of known indicators or malware, such as a file's hash), Signatures which identify known malicious actions, and Heuristics which uses various anomaly detection techniques.

1.2. Protection – Whitelisting

Application Allow listing provides default-deny protection against unknown malware and ransomware on your network. Using our global Allow list, we remote the work that normally comes with Application Whitelisting, a NIST recommended approach. In addition, with the SMART-AV Managed Service, we maintain the Allow list for you if/when someone attempts to install an unknown application. We will review and confirm the application is not malicious and approved for business use before adding to your Allow list.

1.3. RDP Whitelisting

Whitelisting for RDP uses a default-deny approach on each RDP session. RDP authentication easily blocks unknown devices from connecting through RDP inside your network. Any attempts are immediately terminated and logged. It is possible to enable of disable RDP ports, set them on a reoccurring schedule, or temporarily open them for a couple of hours on a specific day. Detailed logging of all RDP sessions provides the ability to quickly review activity including session duration, IP address, location device name, and if the session was blocked or allowed. If a new session is attempted on any device, it can trigger an alert and action to terminate the session, or Allow list that device for the future, or shutdown the machine.

1.4. Endpoint Response Tools

- An integrated VNC agent quick remote access to any managed device.
- Remote CMD enables commands to be sent to an endpoint without a user that is currently at the machine.
- File Manager enables easy file access for incident response, either to download files from the device, or to upload files to needed to correct an issue.
- Reboot & Shutdown are essential capabilities to help with incident containment and eradication, either by preventing the machine from causing more damage, or a change that requires the machine to be rebooted when no one is physically present.

1.5. Reporting

The SMART-AV Customer Portal provides access to dashboards, reports. These reports include operational information about the SMART-AV service, such as details on the Managed Assets, incident information, process execution, custom Allow list/Deny list details, etc. This information can also be exported for additional transformation by the End Customer.

2. SMART-Monitor

The service provides monitoring, detection, alerting and response services to End Customers using CYDEF's cloud-based SMART-Sentinel platform.

2.1. Monitoring

As part of the service, the registered End Customer Assets (Managed Assets) transmit required security data to CYDEF's SMART-Sentinel for processing. The data is normalized and processed to automatically identify expected behavior as well as known malicious or undesirable behavior. Any data that is not matched automatically is investigated by the security operations team and a decision is made.

2.2. Detection

Either through analytics, human validation, or a combination of both, SMART-Monitor will detect undesirable behavior which will be categorized according to its severity and potential impact on the End Customer's environment.

2.3. Alerting

Once undesirable behavior has been identified, CYDEF communicates with the End Customer according to the mechanisms defined in the Communication Alert Matrix. Communications will vary from email notifications, to a combination of emails along with phone calls until an authorized End Customer representative is reached.

2.4. Response

The End Customer can pre-approve isolation/quarantine actions to be taken on behalf of the customer without further approval. These actions include disabling network communications or device shutdown. Additional response capabilities and actions can be provided through additional service agreements.

2.5. Reporting

The Customer Portal provides access to SMART-Monitor dashboards, reports, and access to the data we collect using a search interface. These reports include operational information about the SMART- Monitor service, such as details on the Managed Assets, volume of activity monitored, license management, incident information, etc. This information can also be exported for additional transformation by the End Customer.

3. Roles and Responsibilities

This section describes the roles and responsibilities and uses the following terms:

- Accountable: Delegates work and is the last one to review the task or deliverable before it is deemed complete.
- Responsible: Does the work to complete the task.
- Consulted: Provide input based on their domain of expertise on the work to be performed.
- Informed: Need to be kept in the loop.

3.1. SMART-AV – Managed Service

Responsibilities	CYDEF	Customer
Maintain, monitor, measure the availability and performance of the SMART-AV Customer Portal	RA	I
Respond and resolve to any degradation of Services through the Incident management process.	RA	I
Execute the deployment of anti-malware definitions / pattern file updates / policy configuration / Deny list/Allow list to Managed Assets in scope on a regular basis.	RA	I
Communicate with Client Technical Contact for malware issues that were not resolved automatically.	RA	I
Define requirements for anti-malware protection as defined in the Client Security Configuration Document (CSD).	R	A
Define and maintain Deny lists, Allow lists for anti-malware services.	R	A
Perform ad hoc malware scans on systems as required for security monitoring.	RA	I
Manage, operate, monitor, measure, review and maintain SMART-AV on all Managed Assets in scope.	RA	I
Acknowledge and document rule configuration change requests via the Customer Portal.	RA	I

3.2. SMART-Monitor

Package	Responsibilities	CYDEF	Customer
Essentials	Maintain, monitor, measure the availability and performance of the SMART-Monitor Customer Portal and SMART-Sentinel Cloud components.	RA	I
Essentials	Respond and resolve to any degradation of Services through the Incident management process.	RA	I
Essentials	Execute the deployment of updates to the SMART-Agent (binaries or configuration) to Managed Assets in scope on a regular basis.	RA	I
Essentials	Manage, operate, monitor, measure, review and maintain the SMART-Agent on all Managed Assets in scope.	RA	C
Essentials	Perform investigation of suspicious activity and confirmed security incidents against Managed Assets in scope.	RA	C
Essentials	Communicate with Client Technical Contact for SMART- Monitor incidents that were not resolved automatically as defined in the Client Security Configuration Document (CSD).	RA	I
Essentials	Confirm quality of communications and provide feedback for continuous improvement.	I	RA
Foundations	Acknowledge and document configuration change requests via the Customer Portal.	RA	I
Foundations	Provide read-only access to Customer Data in a searchable format.	RA	I
Foundations	Communicate the severity/priority of a security incident along with forensic details and recommended actions for containment and eradication on Managed Assets in scope.	RA	I

1. Penetration Testing & Vulnerability Assessment

Current industry best practices and standards require penetration testing and vulnerability assessments as part of a mature security program. This is an effective method used to evaluate systems and network security by simulating potential attacks, the same way they would be done by hackers.

This process involves the active analysis of systems to identify their weaknesses and vulnerabilities. The analysis is usually performed from the point of view of a potential attacker and involves the detection and validation of security vulnerabilities, for the purpose of improving the global security of the infrastructures and technological environments.

The type of tests can cover various scenarios such as:

- Attack source: Internal, External, Isolated internal zone, Partner
- Available information: Black box, Grey box, White box
- Testing Environment: Production, Sandbox, Development
- Vulnerability Validation: Scan only, Penetration testing (confirm exploitability)
- Connectivity: Wired or wireless network
- Attack objective: Information theft, Modification of information, Denial of service
- Type of tests: Information security, Physical security, Social Engineering

These activities are managed as projects and we include an engagement manager that will provide oversight and act as the point of contact. All activities are carried out based on the scope of the engagement and require customer approval prior to execution.

2. Incident Response

Depending on their degree of criticality, IT security incidents require an appropriate response, and incident management must be an integral part of an overall security strategy within organizations. The main objective is to avoid or contain the impact of information security incidents to minimize direct and indirect damage to operations. As part of its incident response services, our team of experts intervenes at the Customer's request in each of these phases, in addition to supporting the client's internal communication process. Our methodology explains in more details the actions that will be carried out.

2.1. Diagnosis

When an incident is detected and reported, our experts will diagnose the incident and classify it according to the criteria previously established in the incident management process. They will then determine the appropriate technical procedures to be implemented, as well as those that should not be applied, if any. The level of severity of the incident (impact, urgency, and priority level) will be determined, as well as its scope: which equipment and which services were affected.

In the most severe cases, it is recommended that at least two experts be available to manage an incident, so that one can take the lead to identify and evaluate the incident and the other to help gather preliminary evidence and take mitigating actions. While evidence gathering may occur throughout the process, it will be critical to pay special attention to it at the beginning of the analysis so as not to compromise the integrity of the artifacts.

2.2. Containment

Depending on the nature and circumstances of the incident, the appropriate procedure must be determined and applied, in an established order of priority. The objective is to limit the possible extension of the incident, to confine the damage and restore the service, by looking for the point of entry of the incident. For example, our experts will determine whether the following actions should be carried out, depending on the nature of the incident:

- Disconnection of infected systems
- Modification of firewalls or router filtering rules
- Disabling of access codes and passwords
- Disabling services
- Activating and enhancing logging
- Making backup copies of infected systems
- Collecting evidence
- Documenting the event

Thus, temporary measures will be implemented if required and other specific actions to be taken will be determined and implemented based on circumstances.

2.3. Eradication

When the incident is controlled, the damage is contained, and the evidence has been collected and preserved, the cause of the incident is eliminated as much as possible and operations are returned to normal. More specifically, the following activities will be carried out:

- Retraction of temporary measures
- Elimination of the cause of the incident
- Scan of systems and affected files with anti-malware software to ensure that any latent malware is deleted
- Evidence collection
- Restoration and support plans

At the end of the eradication process, our team ensures that the restoration measures are properly implemented and can coordinate the complete operation for our clients, if required.

2.4. Investigation

In many cases and depending on the severity and nature of the incident, an investigation will be conducted to preserve any evidence that may support a judicial proceeding. To this effect, a seizure of affected equipment will be made to make mirror copies, to analyze them without altering the original data to secure and preserve the integrity of the evidence. Any source of relevant information will be scrutinized and examined to obtain as complete a file as possible in preparation for judicial proceedings. The relevant information for the analysis will then be extracted from the copies, and our experts will analyze the extracted data to identify the cause of the incident or the potential wrongdoers. An investigation will generally take place if a criminal activity is suspected or if litigation is likely to occur, in conjunction with the client's investigation procedures, if any.

2.5. Post-Mortem

Incident analysis is crucial to understanding the circumstances and learning from the experience. At the end of the incident, we prepare a report outlining recommendations for improvements to our client's processes. Each report assists the client in setting up additional or different procedures, as well as in preventing future incidents. In particular, the report addresses the following:

- When was the problem first detected and by whom
- The scope of the incident
- How it was contained and eradicated
- Work done during recovery
- Areas where response teams were less effective
- Areas that need improvement
- Discussion with the teams on how to improve the team. This activity is extremely beneficial for members to share ideas and information to improve team efficiency in future incidents.

3. Strategic Consulting & Expertise on Demand

Whether it is to assist an existing team or to provide specific expertise, our team can intervene at any given stage of a project. We offer support for projects of any size and provides specialized resources, according to customer needs.

4. Computer Forensics

Supported by their experience, training and specialized tools, our certified experts handle the evidence obtained according to best industry practices to ensure its integrity throughout the process of obtaining, duplicating, analyzing, processing and presenting results and protection of evidence.

5. Electronic Evidence Management (eDiscovery)

Electronic Evidence Management refers to the processing and disclosure of evidence in judicial proceedings, particularly where the evidence is complex and voluminous. Since electronic evidence can involve complex legal, technical, and strategic issues, proper planning from the outset can avoid disproportionate costs. The goal is to centralize all relevant documentation in an electronic file for advanced research and ensure that nothing is lost. The management of electronic evidence is done using the Summation software, designed for this purpose and is subject to rules of procedure and processes mutually agreed between the parties. This service can be used to intelligently sort artifacts, search for evidence quickly and efficiently using advanced search options, redact privileged documents, and analyze metadata.