SERVICE STATEMENT

SERVICE STATEMENT

This Service Statement contains provisions that define, clarify, and govern the services described in the quote to which it is attached (the "Quote"). If you do not agree with the terms of this Service Statement, you should not sign the Quote and you must contact us for more information.

This Service Statement is our "owner's manual" that generally describes all managed services provided or facilitated by Westshore Technologies, LLC d/b/a predictiveIT ("predictiveIT"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). Activities or items that are not specifically described in the Quote will be out of scope and will not be included unless otherwise agreed to by us in writing.

This Service Statement contains important provisions pertaining to the auto-renewal of the Services your Quote, as well as fee increases that may occur from time to time. Please read this Service Statement carefully and keep a copy for your records.

IT MANAGED IT SERVICES

IT MANAGEMENT

PIT's IT MANAGEMENT Services include all the documentation, standardization, monitoring, proactive maintenance, and other NOC services necessary to keep your computers, server, and other Technology assets up, running and at peak performance. We standardize your Technology Infrastructure, establish, and follow a customized proactive maintenance plan, and perform 24x7 monitoring of standard & customized critical services, critical events, security events and more.

Our NOC team will perform regular maintenance on your technology systems; to avoid issues that could impact your business, also most maintenance will be performed outside your normal business hours, so it will never impact your business. When our NOC team receives alerts from your systems we will act immediately and remotely connect to the problem system and resolve the issue. IT MANAGEMENT includes the following services:

SITE DOCUMENTATION

A senior engineer will create a **Client Site Document** specifically for your company. Documentation will be stored in electronic format in predictiveIT electronic systems and will hold important information about your technology infrastructure. predictiveIT will provide key client contacts access to or copies of the documentation, but reserves the right to restrict access to any predictive IT specific credentials or information. Site documentation covers important items that are needed for ongoing technology support including:

- Hardware and Software Asset Inventory
- Data Backup Schedules
- ISP and Website information
- Password Inventory for all critical Hardware, Software, and third-party Web Portals
- Patch Management Policy
- Monitoring & Alert Escalation Policy

SERVER MONITORING

This 24x7 monitoring service will allow us to watch your Servers to detect and report problems before they escalate into downtime, data loss, or expensive repair issues. Some of the items we monitor include:

- Operating System/Terminal Server
- Network Services
- Active Directory
- Applications such as Exchange, SQL Server, Citrix
- Critical Event Logs
- Security Event Logs
- Application Status
- System Performance Data
- Backup Monitoring and Administration
- Line of Business-Critical Services & Best Effort Custom Events

Each Client will fill out an Escalation Procedure listing the critical items of your network and your notification preference. A full list of standard monitoring metrics can be found in the "predictiveIT Default Monitoring Policies & Critical Application Monitoring Guide" located on the Client Portal.

SERVER AND WORKSTATION PREVENTATIVE MAINTENANCE

This service allows us to provide preventative maintenance activities on your servers, workstations, and laptops to help prevent problems before they escalate into downtime, data loss, or expensive repair issues. We include the following preventative maintenance services on an ongoing basis including:

- Patch Management (white-listed Critical Security patches for Microsoft operating systems and applications)8
- Regular Performance Review
- Temporary File and Internet Debris Removal
- Hard Drive integrity checks (SMART enabled computers only)
- Service Pack Installation
- Spyware/Malware Removal
- Applications such as Exchange, SQL Server, Citrix

NETWORK DEVICE MONITORING

This 24X7 monitoring service includes availability monitoring for Network Devices such as:

- Local area network IP devices (routers, firewalls, network-enabled printers, etc.)
- Local area network SNMP enabled devices (switches, etc.)
- Gateway VPN tunnels
- Externally hosted web and email servers

SECURITY MONITORING

Our team will monitor several different security components of your technology infrastructure, including workstation & server security event logs, firewall logs, anti-virus logs, spyware logs, remote connection logs and VPN logs. In the event our team discovers a possible threat we will remotely connect to your system and attempt to remediate the issue.

MANAGED BACKUP & DISASTER RECOVERY SERVICES

predictiveIT will monitor supported client or predictiveIT supplied backup and disaster recovery solutions, alert client to backup failure and provide remediation services.
Managed Backup & Disaster Recovery Services include:

- predictiveIT will provide client backup & disaster recovery licenses for all ProCare/EliteCare servers under contract.
- Client is responsible for providing or purchasing backup media such as a Network Attached Storage Device.
- Client is responsible for paying for remote cloud storage for offsite backups.
- predictiveIT will manage clients existing cloud backup solution such as Azure Backups.

MANAGED NEXT-GEN ANTIVIRUS & ANTI-MALWARE PROTECTION

predictiveIT will provide managed Nextgen Anti-Virus & Anti-Malware protection on all covered desktops and servers. PIT NOC team members will monitor the endpoint protection for status, updates and ensure scheduled scans are regularly run.

- PIT's choice of software to provide these services.
- Day to day management of each.

IT SUPPORT

UNLIMITED END-USER HELP DESK TELEPHONE AND REMOTE SUPPORT

Our team of knowledgeable and courteous technicians are available to answer basic questions and solve problems quickly over the phone or through remote support. If, after 30 minutes, the Help Desk Technician has not been able to identify a clear path to resolution, or it is determined that an on-site visit is necessary, we will contact your company's **Authorized Contact**, and if authorized the support issue will be dispatched to a field technician for onsite support.

UNLIMITED REMOTE TIER 2&3 SERVICE DESK SUPPORT

Our secure remote support tool enables us to respond more quickly to problems by accessing your network from our office and eliminating the delay of waiting for an engineer to come on site. If there is an issue that takes advanced technical expertise such as Server, Router, or Firewall configuration or troubleshooting, our Tier 2 & 3 Service Desk team will work remotely to handle your

request. If, after a reasonable amount of time, the Service Desk Technician has not been able to identify a clear path to resolution, or it is determined that an on-site visit is necessary, we will contact your company's **Authorized Contact**, and if authorized the support issue will be dispatched to a field technician for onsite support.

SERVER ADMINISTRATION

Included as part of the Help Desk Telephone and Remote Support service, our technicians will perform a variety of common server administration tasks for no additional fee:

- Create, disable, and maintain user accounts
- Change or reset user account passwords
- Manage security rights and security group memberships
- Create and manage directory shares

MONTHLY REPORTS

Each month we will provide a comprehensive report of the overall health of your technology, plus any issues and repairs experienced over the previous month.

- Executive Summary Report
- Uptime Report
- SLA Report
- System Health Report

ESCALATED LOCAL ONSITE SUPPORT

If you experience any type of problem that cannot be resolved remotely, our team of technicians will troubleshoot and resolve the issue onsite at our current published rate, or at such other discounted rate which client qualifies to receive by this agreement or subsequent fully executed addendum. Excluded are trip and travel expenses.

DISCOUNT OFF HOURLY RATE ON OTHER PROFESSIONAL SERVICES AND OUT-OF-PLAN TECHNICAL SERVICES

Any services provided by predictiveIT that are not explicitly defined under the predictiveIT plan will be billed on a time and materials basis at our current published rate, or at such other discounted rate which client qualifies to receive by this agreement or subsequent fully executed addendum. Excluded are trip and travel expenses. Hardware, software, and products or services provided by 3rd party partners are not eligible for a guaranteed discount at any time.

MONTHLY MAINTENANCE

Managed Services monthly service plans (over $2,000 of Managed IT Services) include a specific number of hours to be used for remote and onsite maintenance. predictiveIT has a prescribed maintenance checklist which is used to ensure that specific maintenance does not result in network downtime. This time is meant to provide adequate time for all maintenance, documentation updates, and assessments when necessary. We encourage our clients to communicate in advance with our Service Desk those items for which attention will be needed. This will allow for the creation of the required ticket(s), and will ensure the technician is properly prepared to address each issue, has the appropriate supplies, tools, etc. PIT will make every attempt to provide notice of any additional time that may be required, and that will exceed client's allotted "block" hours. This allows our clients to prioritize their needs. Each onsite visit will incur a minimum trip charge of $55.00 and as covered under the section titled, "Travel Expenses & Trip Fees".

IT STRATEGY

As part of your predictiveIT Managed Service offering, your company will be assigned a dedicated vCIO (Virtual- Chief Information Officer) who will assist you in setting up and overseeing a strategic technology plan for your company. Your vCIO is tasked with helping your firm become more profitable and efficient through better investment in, and improved utilization of, technology in your business.

QUARTERLY BUSINESS REVIEW

We will use this time to assess your personal comfort level with your current technology, prioritize any outstanding issues, review current and upcoming projects; plan technology needs to support anticipated changes to your business in upcoming months.

- Review Service Activity for the Period
- Prioritize Outstanding Issues
- Review current Project & Upcoming Projects
- Service Satisfaction Questionnaire

RECURRING PROACTIVE MANAGEMENT – TECHNOLOGY ALIGNMENT SERVICES

predictiveIT will assign a Technology Alignment Manager (TAM) to each client account. PIT TAM's will either remotely or onsite perform proactive best practice assessments on a predefined scheduled basis. TAM's will document any discovered issues as well as report any discovered issues to the client primary contact and the clients vCIO. Low – Medium Priority issues will be discussed in the Quarterly Business Review, High – Critical Issues will be reported as soon as they are discovered. TAM's will manage the discovered issues list and document them in Quarterly Action Plans to ensure they are monitored and ultimately remediated. Recurring Proactive Management Services Include:

- Scheduled Proactive Onsite / Remote Best Practice Assessments
- Quarterly Action Plan Management
  - Note: Minor remediations (<1hr) can be performed as part of any of the clients block hours, however some remediations will require the approval and purchase of Professional Services hours and/or Hardware or Software that is not included in this service.

IT PROJECT MANAGEMENT

Your vCIO will provide project management services on small projects, post QBR project tasks, quarterly objectives, and project management of less than 2hrs. For any significant technology projects predictiveIT will provide an assigned project manager and the project management hours will be quoted and billed as part of the project. He or she will provide help determining project costs, set expectations, provide status reports, and oversee employees and/or subcontractors necessary for completing tasks on the project.

VIRTUAL PURCHASING AGENT

Your Virtual Purchasing Agent will assist in researching and providing recommendations about which new hardware and software will help your company achieve greater efficiency. These recommendations include basic hardware specifications through selection of industry-specific software that may help improve corporate performance. Your Virtual Purchasing Agent will also provide updates on the status of warranties, when it is necessary to extend a warranty or consider replacing outdated equipment. This is all in an effort to ensure your devices are in warranty and operating at maximum efficiency by being eligible for the latest manufacture updates. Large projects may require additional consulting services which will be discussed and approved by the client in advance.

TECHNOLOGY BUDGET REVIEW

Your vCIO will provide insight and guidance for budgeting and forecasting your IT infrastructure investments that will help your business avoid unexpected expenses and show you how to properly allocate funds to ensure your infrastructure remains secure, stable, and supportive of your business objectives. This service occurs at the end of each contract year for clients with multi-year agreements of 24 months are greater.

VENDOR & LINE OF BUSINESS MANAGEMENT

PIT takes responsibility for communicating with vendors and line of business software providers to resolve support issues and review your existing contracts to make sure your company is getting the most for your money. You and your users have a single point of contact for all support issues, and you will never hear "it's not our problem" or "it's not the network it's the software", instead we work with your vendors to resolve the issue rather than pointing fingers. Here are some of the categories this service includes:

- Web & Email Hosting Coordination & Support.
- Internet & Phone Circuit Service Provider Coordination & Support
- Copier / Printer Vendor Coordination & Support
- Line of business Software & Hardware Vendor Support Liaison

BASELINE DISASTER RECOVERY PLAN

Disasters come in the form of fires, tornados, hurricanes, earthquakes, floods, hardware failure and even major road closures. To help ensure you're always prepared for the worst, your vCIO will create a basic disaster recovery plan for how your business will recover. Your vCIO can take this plan to the next level, up to and including personal training and complete Business Continuity Plan however, custom Disaster Recovery & Business Continuity Planning will be billable. Unless a plan exists that is regularly maintained and communicated to your team, you are not prepared. This service occurs at the end of each contract year for clients with multi-year agreements of 24 months or greater.

BASELINE SECURITY & RISK ANALYSIS

Your vCIO will review security risks which exist in your current technology infrastructure. The results will be compared with industry best practices, and a risk mitigation and contingency recommendation will be provided. Your vCIO can take this analysis to the next level, up to and including a firm-wide comprehensive security analysis and staff training, for an additional fee. This service occurs at the end of each contract year for clients with multi-year agreements of 24 months or greater.

BASELINE IT & SECURITY POLICIES

Your vCIO will assist in creating the 'IT related' components of your company's policies and employee manuals. These recommendations will be tailored to your business and will provide sound policies on how to protect your firm's investment and the company's most valuable asset, your company's data. This service occurs at the end of each contract year for clients with multi-year agreements of 24 months or greater.

SECURITY & COMPLIANCE SERVICES

24x7x365 SECURITY & NETWORK OPERATIONS (SOC) SERVICES

We are living in a new state of reality that it is not a matter of "IF" you will be attacked but rather "WHEN" you will be attacked. Businesses are constantly under attack by threat actors, automated bots that leverage AI, low cost or free ransomware as a service platform, organized cybercrime groups and nation state funded threat groups. All the above guarantees every business has, or will be under attack. It is impossible to prevent all attacks, so it is imperative that you detect, respond, and mitigate attacks as fast as possible. This is why companies need a team of trained cybersecurity professionals that can detect, respond, and mitigate attacks as quickly as possible. The predictiveIT SOC uses a Security Incident & Event Management Systems (SIEM) to collect Security Events across all the security tools deployed in a client's environment, to correlate all of the various information in one place and using AI, MITRE ATT&CK framework mapping to detect, respond to and mitigate threats in real-time 24x7x365. The predictiveIT Managed SOC Services include:

- 24x7x365 Monitoring, Detection, Response, and Initial Mitigation Services
- Managed Cloud Based SIEM Platform
- Telemetry Agents for Endpoint Isolation on all Covered Devices
- Firewall Integration
- Microsoft 365 and Azure AD Monitoring
- Incident Response Services*
- Remediation Action Plan for Security Incidents
- Computer Isolation on Active Threats
- Monthly Reports

*See Exhibit B Managed SOC Services Scope of Services & SLA for more specific technical information.

MANAGED ENDPOINT PROTECTION, DECTION & RESPONSE SERVICES

Our Security Operations Center (SOC) supported endpoint monitoring and threat detection is designed to identify active threats and remediate attacks. Our SOC technicians will actively monitor and analyze all alerts generated and immediately start remediation steps when confirmed malicious attacks are in progress, including scrubbing the system of any remnant of an attack.

- Constantly monitoring and analyzing your IT environment to effectively protect against threats across endpoints and networks.
- Identifying advanced malware, exploits, and script-based stealth attacks, utilizing attack forensics and intelligent automation.
- Rapidly activating remediation steps when confirmed malicious attacks are in progress, including scrubbing the system of any remnant of an attack, such as malicious processes or registry keys.
- System rollback, in extreme cases, to restore system and data access.

DNS & WEB CONTENT FILTERING

DNS Protection and Web Content Filtering is designed to protect your users from internet threats and websites that contain malicious code. Additionally, DNS Protection can help protect your mobile users while on public and guest Wi-Fi. Our Web Content Filtering has over 80 web categories that can be configured to help protect your employees from visiting dangerous sites and/or non-work-related sites. Our team of security engineers will deploy and configure DNS Protection to all covered desktops, laptops and mobile devices. Once deployed our team will go through a questionnaire with a chosen member(s) of your staff to

determine the best configuration for DNS protection and Web Content Filtering, for your organization. Our team will add all whitelisted websites as well as provide ongoing management.

- Configure Client Specific DNS & Web Content Filtering Portal
- Configure Security Groups and Corresponding Web Filtering Settings
- Add Whitelist/Blacklist Requests
- Schedule Monthly Reports to be sent to designated contacts.

SECURITY AWARENESS TRAINING SERVICES

No matter the size of your business, it is users that are the most heavily targeted by attackers, who know a single phishing email could mean access to everything on your corporate network. Our team will configure the security awareness training system to create ongoing simulated phishing campaigns, as well as configure access for your team to the security awareness training resources.

- Configure Security Awareness Training Portal
- Create Monthly Security Awareness Training Campaigns
- Create & Send Monthly Simulated Phishing Campaigns
- Schedule Monthly Reports to be sent to designated contacts.

VULNERABILITY MANAGEMENT SERVICES

One of the top ways threat actors breach company environments is by exploiting known vulnerabilities. Thousands of new vulnerabilities are discovered and reported by threat research groups and/or manufacturers monthly. These vulnerabilities span across all network devices such as printers, scanners, firewalls, all computers operating systems such as Windows, macOS, ChromeOS and Software that run on your computers such as Microsoft Office, Paint, Adobe, and other Cloud based software. Threat actors exploit these vulnerabilities in order to stage denial of service attacks, gain unauthorized access to your systems, breach data and/or deploy ransomware. The predictiveIT Vulnerability Management Services is designed to detect vulnerabilities across your environment both in the office and on remote worker computers, so that our team can mitigate and ultimately remediate them before they result in a breach.
The SOC Team will:

- Install Network Probes and Light Agents across your environment to actively scan all assets for vulnerabilities.
- Alert on and create tickets for discovered vulnerabilities.
- Create, Maintain, and communicate a Remediation Action Plain
- Recommend and/or assist in remediation of discovered vulnerabilities based on severity.
- Provide Monthly Reports

* The predictiveIT SOC team is constantly developing automated remediation scripts to remediate vulnerabilities across the environment. All manual remediation will either be billed against the clients monthly block contract or as a project.

MANAGED MULTI-FACTOR AUTHENTICATION (MFA) SERVICES

The most common way threat actors gain unauthorized access to critical client systems, resulting in data breaches and ransomware attacks is through compromised or stolen credentials. Threat actors obtain credentials through various ways including but not limited to lists available on the Darkweb, Phishing attacks, legitimate websites that have been hacked and social engineering. Using MFA adds an additional layer of protection on accounts whose credentials have been compromised, by requiring a threat actor to provide an additional code in conjuction with credentials to gain access to an account or resource.

predictiveIT managed MFA services add MFA security to software, cloud services and critical infrastructure in the client's environment.

- Provision and Manage the Clients MFA Portal in predictiveIT's MFA platform.
- Deploy MFA app to all clients protected users via Cell Phone or Token
- Configure MFA for all Administrative accounts on all supported Servers, Networking Infrastructure and Cloud platforms.
- Monitor and respond to all MFA security events.
- Provide Monthly Reports

*Managed MFA includes a basic level MFA software license for each covered user, however in some instances additional MFA licenses may be required where there are tablet users or additional mailbox users, etc. The additional licenses will be charged separately at the client's expense.

DARKWEB MONITORING

The most common way threat actors gain unauthorized access to critical client systems, resulting in data breaches and ransomware attacks is through compromised or stolen credentials. People often use their company email as their username for other business-related apps such as Adobe, Parking Apps, Municipal apps, etc. In addition, people will often use the same password across multiple apps for convenience. The combination becomes extremely dangerous when these online services get breached and credentials are stolen, because threat actors will then collect all those credentials and sell them on Darkweb. Additionally, bots, automated phishing and social engineering campaigns steal user credentials constantly and these credentials are sold on the Darkweb as well. There is a huge buying market for stolen credentials as it provides threat actors a cheap and easy way to gain initial access and launch a much more lucrative data breach or ransomware attack.

predictiveIT Darkweb Monitoring, monitors the Darkweb sites that broker in stolen credentials for credentials containing the clients covered domain name. If we identify credentials relating to a client's organization, we notify the client of the existence of credentials and if possible, the specific password compromised, and/or source of the breach. predictiveIT Darkweb Monitoring Services Include:

- Darkweb Monitoring for Client Business Domain Names and Key Executives Personal Email Accounts
- Notification of discovered compromised credentials and if possible, the source of breach information.
- Monthly Reports

PRIVILEDGE ACCESS MANAGEMENT (PAM) SERVICES

predictiveIT Security Engineer's will perform annual security risk assessments to identify risk, likelihood of risk and document discovered issues. PIT will provide clients with a copy of discovered issues along with remediation recommendations. Remediation may require the purchase of Professional Services Hours, Additional Services, Software and/or Hardware.

CLOUD & SaaS MONITORING & PROTECTION SERVICES

Cloud and Software as a Service (SaaS) based applications have changed the way businesses define productivity making it easier and much more productive by providing access to business applications and data anywhere anytime. However, those same features also make it easier for threat actors to launch attacks from anywhere, anytime and go unnoticed after they compromise your systems. The ease and occurrences of successful cyber-attacks against cloud and SaaS based applications has exponentially gone up year over years with the ability to detect attaches and/or breaches becoming a lot harder due to the distributed nature of these applications.

The predictiveIT Managed Cloud & SaaS Protection Services ties into common Cloud and SaaS platforms such as Microsoft 365, AzureAD, Google G-Suite, Salesforce and more to monitor, detect and mitigate attacks. Our SOC monitors over 300 different event criteria, to detect threats, Indicators of Compromise (IOCs) and breaches. The SOC team is constantly tuning automated response rules that can prevent attacks and stop breaches before they happen. From detecting failed logons, logons from foreign countries to data loss prevention, our team is protecting your critical Cloud & SaaS based applications. predictiveIT's Cloud & SaaS Protection Services include:

- 24x7x365 Monitoring & Response for Covered Cloud and SaaS Based Applications
- Cloud/SaaS Protection License for each Covered User
- Monthly Reporting & Analysis

ANTI-SPAM / ANTI-PHISHING PROTECTION

Businesses receive millions of phishing emails per year, with many of them being extremely effective at making the target take action, whether that be clicking a link, opening attachment, sending money and/or entering in credentials into a malicious website. With AI, the effectiveness of phishing has increased exponentially, and businesses can no longer count on grammar mistakes, formatting issues or obviously fake emails to mitigate attacks.

predictiveIT Email Protection Services uses a combination of AI, Machine Learning, and end user feedback to screen emails to and detect phishing and/or other email-based attacks. Along with industry leading Anti-spam and Anti-Malware protection, our email protection services also identify phishing attacks. When a suspicious email is detected, a banner is placed in the email to notify the user to beware. The banner will include the reasons why our protection systems flagged the email as suspicious. predictiveIT Email Protection Services include:

- 24x7x365 Monitoring & Response Services
- Email Protection Licenses for each covered user
- Monthly Reporting & Analysis

ITEMS NOT COVERED

The following items are excluded from the predictiveIT Support Plan:

- Support or Onsite Professional Services are defined as all services performed onsite other than those covered by the "Proactive & Escalated Onsite Services Blocks" and approved ELITECARE Escalated Support.

Travel Expenses & Trip Fees

All onsite visits will incur related travel, mileage, or trip fees. The fees are to cover mileage reimbursements to PIT technicians and administrative costs. PIT bills travel expenses in one of the following ways:

1. $55 Flat Trip Charge per day for travel to any Client location within a 50-mile radius of the PIT office closest to the Client location we are traveling to.
2. $0.75/mile travel charge per day, for round trip travel from our office to Client location, and back. This applies to any travel to a Client location exceeding a 50 miles radius of the PIT office closest to the Client location.

In addition, PIT reserves the right to charge Client all reasonable travel expenses including airfare, lodging, rental car fee, etc., when necessary, as discussed and approved by Client.

Hardware and Software

The cost of any hardware or software will be billed in addition to your service plan, including:

- Hardware and/or software required to troubleshoot and resolve break/fix issues
- Hardware upgrades to covered equipment.
- Software upgrades to covered operating systems and business applications
- New hardware, software, or other equipment

Installation of New Hardware, Software, and Other Equipment

Services required to research, select, and implement new hardware, software, and other equipment will be billed hourly at clients discounted hourly rate. Once implemented, the maintenance of new hardware, software, and other equipment will be incorporated into your PIT Managed Services plan provided additional equipment falls within the parameters in this agreement. Provided 48-hour advanced notice is provided to PIT, a flat "New User Set Up Fee" bill be added to all tickets for $200.00, and associated monthly recurring charges will be adjusted accordingly starting with the next billing cycle. It is the client's responsibility to notify PIT when there are user additions or reductions to ensure accurate billing.

Move, Adds and Changes to User Accounts

Provided advance 48-hour notice is provided, a flat "New User Set Up Fee" bill will apply at $125.00, and associated monthly recurring charges will be adjusted accordingly, starting with the next billing cycle. If new equipment is being deployed, time will be billed at T&M rates as defined in this agreement. It is the client's responsibility to notify PIT of any user change to assure accurate billing. PIT will conduct periodic audits and will provide adjusted to monthly recurring charges. Usage is determined by user log-in activity within the past 30 days but will not include service accounts, 3rd party maintenance accounts for which no support is required. Individual existing user moves, performed remotely on existing equipment, is covered under this agreement and at no additional cost.

Non-Supported Software and Equipment

predictiveIT cannot effectively manage the performance of your network and individual systems when new software and equipment is installed without our knowledge and participation. Software and equipment not explicitly listed in Exhibit F of this document will not be covered unless the software or equipment is pre-approved and installed with the participation of a predictiveIT' senior technician.

Problems Caused by Non-Supported Software and Equipment

Resolution of problems caused by non-covered software or equipment will be billed on a time and materials basis at our current published rate, or at such other discounted rate which client qualifies to receive, and as outlined in this agreement or subsequent fully executed addendum plus standard mileage fees. (see appropriate section). All Antivirus and Malware removal services will be billed at T&M rates if users are found to be running as a Local Administrator of the workstation or laptop. predictiveIT encourages users to run as Power Users on their Local Computers and Laptops, as it is impossible for Antivirus Software, Anti-Malware, and other protection software to be effective.

ice, Network or Equipment Relocation

Server, workstation, and printer moves will be billed on a time and materials basis at our current published rate, or at such other discounted rate which client is entitled to per this agreement.

EXHIBIT A – MANAGED IT SERVICES GENERAL SERVICES LEVEL AGREEMENT

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis; response, repair, and/or remediation services (as applicable) will be provided only during business hours unless otherwise specifically stated in the Quote. We will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described below. Severity levels will be determined by predictiveIT in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; predictiveIT will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

<table>
<tr><th></th><th>Response Time[1]</th><th>Normal Business Hours
Monday – Friday, 8 AM to 5 PM</th><th>Extended Hours[2]
Holidays, Non-Normal Business Hours</th></tr>
<tr><td>Chat</td><td>Live Chat</td><td rowspan="2">A technician will respond, on average, in less than 3 minutes of initiating a chat session or phone call during predictiveIT's normal business hours.
For contact initiated during normal business hours, a technician will begin working on the issue immediately subject to technician availability.
If an issue is not resolved during normal business hours, it will be logged and continued the following day.
For contact initiated outside of normal business hours, a ticket will be logged, and work will begin on the next business day.
For non-critical issues where a person is required onsite, we will schedule an engineer for an onsite visit in accordance with the severity of the problem and, always subject to technician availability.</td><td rowspan="2">A technician will respond, on average, in less than 2 hours of initiating a phone call any time, or day of week.
A technician will begin working on the issue immediately subject to technician availability.
For non-critical issues where a person is required onsite, we will schedule an engineer for an onsite visit in accordance with the severity of the problem and, always subject to technician availability.[4]</td></tr>
<tr><td>Phone</td><td>Live Answer</td></tr>
<tr><td>Email / Support Portal</td><td>2-24 Hours</td><td colspan="2">Email support is for non-critical requests.
Response time will vary from 2 hours to 24 hours depending on Severity & Technician availability.
Examples of non-critical requests are:
Software installation
Issues for which a workaround has been implemented.
Frequently asked questions (FAQ)-type requests
Adding / Deleting users
General consulting questions</td></tr>
</table>

[1] **Response time is calculated from the time that the request for help is received by us though our designated support channels. Requests received in any other manner may result in delays or non-responses.**

[2] **Extended Hours are not included. If Extended Hours support is provided, Client will be billed for such support at two times (2x) our then-current hourly rates, with a minimum of one (1) hour. All partial hours after the first hour are billed in fifteen (15) minute increments, with partial increments billed to the next higher increment.**

TROUBLE / SEVERITY	RESPONSE TIME
Critical: Service not available (*e.g.*, all users and functions unavailable)	Response within two (2) business hours after notification.
Significant Degradation (*e.g.*, large number of users or business critical functions affected)	Response within four (4) business hours after notification.
Limited Degradation (*e.g.*, limited number of users or functions affected, business process can continue).	Response within eight (8) business hours after notification.
Small Service Degradation (e.g., business process can continue, one user affected).	Response within two (2) business days after notification.

*All time frames are calculated as of the time that predictiveIT is notified of the applicable issue / problem by Client through predictiveIT's designated support portal, help desk, or by telephone at the telephone number listed in the Quote. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts. Help desk support provided outside of our normal support hours will be billed to Client at the rate (2 hour minimum applies).

Service Credits: Our service level target is 90% as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Client timely brings that failure to our attention in writing (as per the requirements of the MSA), then Client will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote.

EXHIBIT B – MANAGED 24X7X365 SOC SERVICES SCOPE & SERVICES LEVEL AGREEMENT

The below Exhibit covers the Scope of Services and Services Level Agreement included with the predictiveIT Managed SOC Services offering. The below covers more technical details and Service Level Agreements (SLA) for the specific services.

Introduction

PIT SOC team works on the CLIENT's behalf to detect, respond, and remediate critical cybersecurity incidents via all tools and methods available. The arsenal of the PIT's incident response team is constantly adapting to global threat patterns by developing new apps and integrations that blend machine and human learning & actions. The dual automated and manual approach provides a redundant layer of action to effectively detect, investigate, contain, report, and recover.

We base our incident response model on the National Institute of Standards and Technology (**NIST**) Framework of Improving Critical Infrastructure Cybersecurity and the **MITRE ATT&CK®** Framework, among others. The frameworks enable organizations to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. It provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in the industry today.

AREAS OF RESPONSIBILITY

Based on the NIST model we summarize the areas below that depict responsibilities of PIT and the CLIENT to ensure the most effective ability to **DETECT**, **RESPOND**, and **RECOVER** to a cyber event.

FUNCTION	RESPONSIBLE ENTITY	CATEGORY
IDENTIFY	CLIENT / IT PARTNER	Asset Management
	CLIENT / IT PARTNER	Business Environment
	CLIENT / IT PARTNER	Governance
	CLIENT / IT PARTNER	Risk Assessment
	CLIENT / IT PARTNER	Risk Management Strategy
	CLIENT / IT PARTNER	Supply Chain Risk Management
PROTECT	CLIENT / IT PARTNER	Identity Management, Authentication & Access Control
	CLIENT / IT PARTNER	Awareness and Training
	CLIENT / IT PARTNER	Data Security
	CLIENT / IT PARTNER	Information Protection Processes and Procedures
	CLIENT / IT PARTNER	Maintenance
	CLIENT / IT PARTNER	Protective Technology
DETECT	PIT SOC	Anomalies and Events
	PIT SOC	Security Continuous Monitoring
	PIT SOC	Detection Processes
RESPOND	PIT SOC	Response Planning
	PIT SOC	Communications
	PIT SOC	Analysis
	PIT SOC	Mitigation/Remediation
	CLIENT / IT PARTNER	Mitigation/Remediation
	PIT SOC	Improvements
	CLIENT / IT PARTNER	Improvements

RECOVER	**CLIENT / IT PARTNER**	**Recovery Planning**
	CLIENT / IT PARTNER	**Improvements**
	CLIENT / IT PARTNER	**Communications**

DETECTIONS

A threat event has the potential for causing consequences or impact. Events include unauthorized access to computers, unauthorized use of system privileges and execution of malware that destroys, encrypts a system, or steals data. Think of an event as an observable occurrence, such as when a failed login to a computer occurs. While this could be either unintentional or intentional, both are considered events.

A security incident is a violation or imminent threat of security policies or industry best practices. Incident examples include:

- **Denial of service** – an attacker sends high volumes of connection requests to a server, resulting in a crash.
- **Phishing** – employees are enticed to click and open email attachments or links resulting in some form of malware or establishes a connection with external systems.
- **Malware** – Type of application designed to perform a variety of malicious tasks: create persistent access, spy on the user, create disruption, etc. The most notable form of Malware is Ransomware.
- **Ransomware** – an attacker obtains unauthorized access, encrypting the system and asking for a financial sum of money before the computer is decrypted and operational.
- **RDP hijacking** - involves the attacker "resuming" a previously disconnected RDP session. This allows the attacker to get into a privileged system without having to steal the user's credentials.
- **PowerShell** - Attackers commonly use command and script interpreters such as PowerShell to execute malicious commands, run scripts, and binaries when carrying out an attack.
- **PowerShell without PowerShell** – PowerShell commands and scripts can be executed by loading the underlying System.Management.Automation namespace. As a result, this eliminates the need to spawn powershell.exe.
- **Business Email Compromise (BEC)** – an attacker has gained unauthorized access to an employee's email.
- **Man-in-the-middle attack (MITM)** – attacker intercepts the communication between two parties to spy on the victims, steal personal information or credentials, or alter the conversation in some way.
- **Zero-day exploit** – Cyber-criminals learn of a vulnerability that has been discovered in certain widely-used software applications and operating systems, and then target organizations who are using that software to exploit the vulnerability before a fix becomes available.
- **Cryptojacking** – Cyber criminals compromise a user's computer or device and use it to mine cryptocurrencies,
    - such as Bitcoin.
- **DNS Tunnelling** – Is a sophisticated attack vector that is designed to provide attackers with persistent access to a given target. Since many organizations fail to monitor DNS traffic for malicious activity, attackers can insert malware into DNS queries (DNS requests sent from the client to the server). The malware is used to create a persistent communication channel that most firewalls are unable to detect.
- **Drive-by Attack** – A 'drive-by-download' attack is where an unsuspecting victim visits a website which in turn infects their device with malware. The website in question could be one that is directly controlled by the attacker, or one that has been compromised. In some cases, malware is served in content such as banners and advertisements. These days exploit kits are available which allow novice hackers to easily set up malicious websites or distribute malicious content through other means.
- **Eavesdropping attack** – Sometimes referred to as "snooping" or "sniffing", an eavesdropping attack is where the attacker looks for unsecured network communications to intercept and access data that is being sent across the network. This is one of the reasons why employees are asked to use a VPN when accessing the company network from an unsecured public Wi-Fi hotspot.

CYBER THREAT INTELLIGENCE

One of the approaches we follow is MITRE ATT&CK Mapping to help us understand adversary behavior as a first step in protecting networks and data. The MITRE ATT&CK® framework is based on real-world observations and provides details on 100+ threat actor groups, including the techniques and software they use. It helps identify defensive gaps, assess security tool capabilities, organize detections, hunt for threats, or validate mitigation controls.

ATT&CK describes behaviors across the adversary lifecycle, commonly known as tactics, techniques, and procedures (TTPs). These behaviors correspond to four increasingly granular levels:

- **Tactics** represent the "what" and "why" of an ATT&CK technique or sub-technique. They are the adversary's technical goals, the reason for performing an action, and what they are trying to achieve. For example, an adversary may want to achieve credential access to gain access to a target network. Each tactic contains an array of techniques that network defenders have observed being used in the wild by threat actors.
- **Techniques** represent how an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. Techniques may also represent what an adversary gains by performing an action. A technique is a specific behavior to achieve a goal and is often a single step in a string of activities intended to complete the adversary's overall mission.
- **Sub-techniques** provide more granular descriptions of techniques. For example, there are behaviors under the OS Credential Dumping technique that describe specific methods to perform the technique. Sub-techniques are often, but not always, operating system or platform specific. Not all techniques have sub-techniques.
- **Procedures** - how a technique or sub-technique has been used. They can be useful for replication of an incident with adversary emulation and for specifics on how to detect that instance in use.

The steps we follow are:

- **Find the behavior**. Searching for signs of adversary behavior is a paradigm shift from looking for Indicators of Compromise (IOCs), hashes of malware files, URLs, domain names, and other artifacts of previous compromise. The PIT SOC Agent is collecting signs of how the adversary interacted with specific platforms and applications to find a chain of anomalous or suspicious behavior prior to damaging the customers' business.
- **Research the Behavior**. Additional research may be needed to gain the required context to understand suspicious adversary or software behaviors. Use additional resources integrated with PIT SOC's platform and/or external resources when needed, to gain information on the potential threat.
- **Identify the Tactics.** Comb through the report to identify the adversary tactics and the flow of the attack. To identify the tactics, we focus on what the adversary was trying to accomplish and why. Was the goal to steal the data? Was it to destroy the data? Was it to escalate privileges?
- **Identify the Techniques**. After identifying the tactics, review the technical details associated with how the adversary tried to achieve their goals. For example, how did the adversary gain the Initial Access foothold? Was it through spear-phishing or through an external remote service? Drill down on the range of possible techniques by reviewing the observed behaviors in the report.
- **Identify the Sub-techniques**. Review sub-technique descriptions to see if they match the information in the report. Does one of them align? If so, this is probably the right sub-technique. Depending upon the level of detail in the reporting, it may not be possible to identify the sub-technique in all cases. Read the sub-technique descriptions carefully to understand the differences between them. For example, Brute Force includes four sub- techniques: Password Guessing, Password Cracking, Password Spraying, and Credential Stuffing.
- Take or recommend remediation steps depending on the identified threat(s).

EVENT DATA COLLECTION, ANALYSIS AND TRIAGE (DETECT)

Triage is the investigation of a threat event, resulting in a verdict of malicious, suspicious, or benign. Events defined as malicious or suspicious are considered an incident. Events are generated throughout the day and span networks, endpoints (computers) and cloud applications.

The PIT SOC utilizes multiple cyber intelligence feeds that help enhance many of the services below to detect new emerging threats. The PIT SOC agent provides continuous monitoring for suspicious or malicious behavior and presents these findings in data that can be actioned through automation or human analysts.

Below is a list of ever evolving services that the PIT SOC Platform and SOC team are constantly monitoring, triaging, and responding to. Should a serious threat be found, the PIT SOC agent can isolate the device from the rest of the network. This allows further investigations without exposing threats to the rest of the customer systems.

APP	DETECT
ADVANCED BREACH DETECTION	The PIT SOC Agent identifies computers that are compromised where security defenses have been circumvented. Malicious activity reported by our SOC agent requires immediate investigation.
CRYPTO MINING DETECTION	The PIT SOC Agent detects crypto mining activity form browser based crypto miners as well as common crypto mining client software.
CYBER TERRORIST NETWORK CONNECTIONS	The PIT SOC Agent detects network connections to various nation states that have been known to engage in cyberterrorist activities and malicious network activity such as backdoor connections to C2 servers and malicious systems.
ENDPOINT EVENT LOG MONITOR	The PIT SOC Agent monitors the Microsoft Windows or macOS Event Log for suspicious events. Detected events are security related activities such as failed logins, clearing security logs, unauthorized activity, etc.
FIREWALL LOG ANALYZER	The PIT SOC Agent acts as a syslog server collecting log messages from edge devices on your network. Messages are parsed and analyzed for potential threat indicators. When a potential threat or security related event is detected, it will forward the detection to the Cloud Console.
MALICIOUS FILE DETECTION	The PIT SOC Agent monitors and detects suspicious and malicious files that are written to disk or executed.
MICROSOFT EXCHANGE HAFNIUM EXPLOIT DETECTION	The PIT SOC Agent will look for specific Indicators of compromise (IOCs) related to exploitation of Microsoft Exchange 2010, 2013, 2016 and 2019 via CVE CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. It will also report the patch status for mitigations against these vulnerabilities.
OFFICE 365 LOGIN ANALYZER	Detects logins outside the expected countries or known malicious IP addresses
OFFICE 365 LOG MONITOR	The SOC Platform ingests and reports on Microsoft Office 365 and Azure log data.
OFFICE 365 RISK DETECTION	We focus on the riskiest accounts, users, and behaviors. Determined risk through a combination of industry heuristics and machine learning.

OFFICE 365 SECURE SCORE	Overall description of cloud security posture with itemized remediation plans across all Office365 tenants.
SUSPICIOUS NETWORK SERVICES	The PIT SOC Agent detects suspicious network services running on an endpoint. While there are 65,535 available network services for legitimate use, suspicious detections are defined as well-known ports and services that are leveraged for malicious intent.
SUSPICIOUS TOOLS	The PIT SOC Agent detects programs that can negatively impact the security of the system and business network. Detected suspicious tools should be investigated and are categorized as hacking utilities, password crackers, or other tools used by attackers for malicious purposes.
SENTINELONE MONITOR	The SOC Platform ingests and reports on detections from SentinelOne. The integration allows the SOC to trigger action from SentinelOne installed on endpoint to kill, quarantine, remediate, rollback, and to disconnect device from network.

INCIDENT RESPONSE (RESPOND)

The threat landscape and attacker's techniques are constantly evolving. While it is not feasible to list every attack and response scenario, the tables below outline common attack techniques and the anticipated actions of the PIT SOC team and the CLIENT. While the list is not exhaustive, please use this as a guideline of what to expect when incidents are detected via the PIT SOC platform.

When calling, the SOC will call all available numbers in the Notifications section. If a **critical threat** to a business system is detected, the SOC manager will authorize taking the device offline to stop the spreading of the threat even in the event when no one can be reached, unless otherwise specified by the IT Partner. The SOC will continue to call the available numbers until a team member of our IT Partner is reached. We consider every Incident that requires a phone call from the SOC to the CLIENT a Severity 1 case.

Upon generation of an event that is classified as an incident, the RSOC team will begin investigation within minutes of detection and will provide update within the given timeframe. This is measured by taking the difference between creation of the incident as shown in the audit log and when the incident is either assigned to a RSOC analyst or manually escalated.

SEVERITY LEVELS - INCIDENTS			
Severity	**Impact**	**Definition**	**SLA**
SEV 1	Critical	System, its files, and/or functions are breached, exfiltrated, changed, deleted, or otherwise compromised.	**90 Minutes**
SEV 2	Major	System is under attack but no breach by malicious party was successful, and no system components were compromised.	**24 Hours**
SEV 3	Minor	System is showing failed logon attempts or other events generated by customer network systems or users and not part of a cybersecurity threat.	**72 Hours**
SEV 4	Informational	No effect on the system is recorded.	**72 Hours +**

ADVANCED BREACH DETECTION				
DETECT	**ANALYZE**	**REMEDIATION / MITIGATION**		**NOTIFICATION**
PIT SOC	**PIT SOC**	**PIT SOC**	**CLIENT / IT PARTNER**	**PIT SOC**

SUSPICIOUSLY SIGNED BINARY PROXY EXCUTION	Analyze file execution. Review timeline of file execution.	If execution malicious, notify CLIENT. Disconnect device from network.	Review the file and remove if not needed. Run a full AV scan. Change any admin passwords with access to machine.	EMAIL CALL
		If execution suspicious, notify CLIENT.	Review event and whitelist if execution is authorized	EMAIL
INHIBIT SYSTEM RECOVERY DETECTED	Analyze executions of vssadmin.exe, wbadmin.exe, or bcdedit.exe	If executions are preceded and/or followed by other suspicious actions, notify CLIENT. Disconnect device from network.	Review the detection. If not authorized, run a full AV scan of the system and other clean-up tools available. Change any admin passwords with access to machine.	EMAIL CALL
		If executions are only suspicious, notify IT PARTNER.	Review the detection. If not authorized, run a full AV scan of the system and other clean-up tools available.	EMAIL

MALICIOUS FILE DETECTION				
DETECT	**ANALYZE**	**REMEDIATION / MITIGATION**		**NOTIFICATION**
PIT SOC	**PIT SOC**	**PIT SOC**	**CLIENT / IT PARTNER**	**PIT SOC**
MALICIOUS FILE DETECTION	Investigate if single file or multiple file execution(s).	If confirmed malware: Notify CLIENT. Disconnect device from network.	Remove entries from Registry. Run AV scan, Malwarebytes Free/Premium, Microsoft MSRT. Remove remaining malicious files manually.	EMAIL CALL
		If suspicious execution but not confirmed as malware: No SOC remediation. Notify CLIENT.	If confirmed malware: Remove entries from Registry. Run AV scan & Malwarebytes Free/Premium. Remove remaining malicious files.	EMAIL
SUSPICIOUS FILE DETECTION	Test file using threat intelligence.	The file XXXXX.exe was flagged as suspicious on device XXXXX Investigate if single file or multiple file execution(s).	Please review and verify the file. Remove if not required. Run a full AV scan on the system. Make sure the system is fully patched. Whitelist if appropriate	EMAIL CALL

CYBER TERRORIST NETWORK CONNECTIONS				
DETECT	**ANALYZE**	**REMEDIATION / MITIGATION**		**NOTIFICATION**
PIT SOC	**PIT SOC**	**PIT SOC**	**CLIENT / IT PARTNER**	**PIT SOC**
SUCCESSFUL MALICIOUS	Test Remote IP using threat intelligence.	No successful login detected: Notify CLIENT. Disconnect device from network.	Place RDP behind VPN. Make sure system is fully patched. Implement strict firewall policies to reduce the attack surface. Consider implementing geo-based policies if applicable.	EMAIL

RDP SESSION	If logon attempted from country in high-risk category	If successful login detected: Notify CLIENT.	Place RDP behind VPN. Fully patch system. Implement strict firewall policies to reduce the attack surface. Consider implementing geo-based policies if applicable.	EMAIL CALL
INBOUND CONNECTIONS FROM xx ON 445 or 25	Inbound connections were detected on port 445 or 25.	If successful logins detected: Notify CLIENT. Identify if any other executions took place.	Block port 445 at the firewall. Implement strict firewall policies to reduce the attack surface by limiting both inbound and outbound traffic to only necessary ports and protocols.	EMAIL CALL
		I failed logins detected: Notify CLIENT	Block port 445 at the firewall. Implement strict firewall policies to reduce the attack surface by limiting both inbound and outbound traffic to only necessary ports and protocols. Remove any files or registry entries Remove any entries from Registry. Run AV scan, Malwarebytes Free/Premium, Microsoft MSRT. Remove remaining malicious files manually.	EMAIL

AV MONITOR				
DETECT	**ANALYZE**	**REMEDIATION / MITIGATION**		**NOTIFICATION**
PIT SOC	**PIT SOC**	**PIT SOC**	**CLIENT / IT PARTNER**	**PIT SOC**
MONITOR: - SENTINELONE	Determine if threat was mitigated – if not, notify CLIENT.	Investigate any other potentially malicious events.	Review the detection. Run a full AV scan of the system and anti-malware utility. Delete registry keys and programs that may have been installed. Whitelist if appropriate.	EMAIL CALL
	Determine if threat was mitigated – if yes, notify CLIENT.	No action.	Review the detection. Run a full AV scan of the system. Whitelist if appropriate.	EMAIL

OFFICE 365 LOGIN ANALYZER				
DETECT	**ANALYZE & COMMUNICATE**	**REMEDIATION / MITIGATION**		**NOTIFICATION**
PIT SOC	**PIT SOC**	**PIT SOC**	**CLIENT / IT PARTNER**	**PIT SOC**
SUSPICIOUS SUCCESSFUL OFFICE 365 LOGIN DETECTED	The following account successfully logged in from country X. Detected logins outside the expected countries or from known malicious IP addresses.	Expected Behavior? Notify CLIENT.	Whitelist the alerts for users from detected location. From Incident View, click on Action/Whitelist to whitelist.	Email
		Unexpected Behavior? Notify CLIENT.	Kill Existing Sessions. Enable 2 Factor Authentication for all users in the Tenant. Add Conditional Access Policies to block by undesired logon regions.	Email CALL

EMAIL FORWARDING RULE DETECTED	Forwarding rule detected to email outside of corporate domain.	Notify CLIENT.	Review the rule. Remove if not authorized. Whitelist if authorized.	Email CALL
O365 LICENSE	The current Office 365 configuration does not allow monitoring of Office 365 Logins for this customer.	Without the proper licensing, the SOC will not be able to monitor for suspicious login activity. Notify IT PARTNER.	The Tenant requires at least one Azure P1 or P2 license to access login data. Follow instructions provided to add the required license.	Email
OFFICE 365 BRUTE FORCE ATTEMPT	Multiple failed logon attempts from various countries; the account is locked.	Notify CLIENT.	Enable 2 Factor Authentication for all users in the Tenant. Add Conditional Access Policies to block undesired logon regions. Kill Existing Sessions.	Email

SUSPICIOUS TOOLS				
DETECT	**ANALYZE**	**REMEDIATION / MITIGATION**		**NOTIFICATION**
PIT SOC	**PIT SOC**	**PIT SOC**	**CLIENT / IT PARTNER**	**PIT SOC**
SOCIAL ENGINEERING TOOLS DETECTED	A suspicious tool classified as Social Engineering Tools was detected.	Review the history for the device. Notify CLIENT.	Review the tool detection. Remove / uninstall if not authorized. Run a full AV scan on the system. Whitelist if appropriate	Email
SUSPICIOUS TOOL: BITCOIN MINING	Investigate if the bitcoin-mining tool is suspicious or authorized.	Review the history for the device. Notify CLIENT.	Review the tool detection. Remove / uninstall if not authorized. Run a full AV scan on the system. Whitelist if appropriate.	Email
SUSPICIOUS TOOL(S) DETECTED: NMAP, WIRESHARK	Investigate if the utility tool detected is suspicious or authorized.	Review the history for the device. Notify CLIENT.	Review the tool detection. Remove / uninstall if not authorized. Run a full AV scan on the system. Whitelist if appropriate	Email

AUTOMATED REMEDIATION (RESPOND)

Device Isolation - PIT SOC can isolate machines on a customer's network that have a PIT SOC Agent installed. The RSOC uses host isolation to prevent the spread of malicious code by preventing a compromised machine from communicating to other network devices on the Internet or the Customer's network. The isolated machine will maintain connectivity to RSOC and allow our analysts to continue investigation without risking other network devices to malicious code or active attacks. Unless the Customer opts-out, PIT SOC will isolate potentially compromised machines. PIT SOC will manually isolate the machine using the installed SOCAgent

and notify the customer of the isolation via an incident for escalation. The machines will remain in isolation until the threat has been remediated or the customer has specifically said they accept the risk and request the RSOC to remove the isolation.

Automated Remediation - For certain incidents, the SOCAgent can perform automated remediation tasks. These remediation actions are visible in the Incident view by clicking the Remediate Action. Customers can opt-in to allow the SOC Analysts to execute the automated remediation actions on affected endpoints. The current remediation actions that can be performed are:

- Terminate Processes
- Remove Files
- Uninstall Programs
- Modify Registry Keys
- Stop Services
- Remove Scheduled Tasks

Antivirus Actions - Some AV Product integrations with the RCC allow RSOC Analysts to perform AV related actions such as Quarantine, Kill, Remediate and Whitelist. The following guidelines apply to integrations that support those features.

- Active Threats (Those not killed, quarantined, or remediated) automatically by the AV agent will be reviewed. Hashes will be verified using various threat intel sources. If found to be benign the RSOC analyst will whitelist. If found to be malicious or unknown the RSOC team will quarantine. If AV Product supports classifications by an RSOC Analysts, the file will be classified as determined by the analyst. An incident will be generated indicating the status of the threat and the action taken by the RSOC analyst.
- Suspicious Threats (Those reported, but not killed, quarantined, or remediated) automatically by the AV agent will be reviewed. Hashes will be verified using various threat intel sources. If found to be benign the SOC team will whitelist. If found to be malicious or unknown the RSOC team will quarantine. If AV Product supports classifications by an RSOC Analysts, the file will be classified as determined by the analyst. An incident will be generated indicating the status of the threat and the action taken by the RSOC analyst.
- All other threats (killed, quarantined, or remediated) automatically by the AV agent will be reported as an incident for customer review and notification.
- Temp files that are detected but not (killed, quarantined, or remediated) automatically by the AV agent will be investigated using best efforts and threat intelligence sources. Incidents will only be generated if the file can be positively identified by the RSOC analyst.
- Other non-file-based threat detections by AV products such as Lateral Movement. An incident will be generated indicating the status of the threat.

RECOMMENDED MITIGATIONS

CISA and FBI recommend that network defenders consider applying the following best practices to strengthen the security posture of their organization's systems whenever feasible:

- Provide social engineering and phishing training to employees.
- Consider drafting or updating a policy addressing suspicious emails that specifies users must report all suspicious emails to the security and/or IT departments.
- Mark external emails with a banner denoting the email is from an external source to assist users in detecting spoofed emails.
- Implement Group Policy Object and firewall rules.
- Implement an antivirus program and a formalized patch management process.
- Implement filters at the email gateway and block suspicious IP addresses at the firewall.
- Adhere to the principle of least privilege.
- Implement a Domain-Based Message Authentication, Reporting & Conformance validation system.
- Segment and segregate networks and functions.

- Limit unnecessary lateral communications between network hoses, segments, and devices.
- Consider using application allowlisting technology on all assets to ensure that only authorized software executes, and all unauthorized software is blocked from executing on assets. Ensure that such technology only allows authorized, digitally signed scripts to run on a system.
- Enforce multi-factor authentication.
- Enable a firewall on agency workstations configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Implement an Intrusion Detection System, if not already used, to detect C2 activity and other potentially malicious network activity
- Monitor web traffic. Restrict user access to suspicious or risky sites.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against network propagation modules used by TrickBot.