PTAAS FLEX POWERED BY REDSPY365 - SERVICE GUIDE

Last Modification Date: 02/12/2024
Exported and Shared on: 03/18/2024

For additional information, visit www.intervision.com

CONTENTS

CUSTOMER and InterVision. ("InterVision") agree that the following defines the services ("Services") to be performed by RedSpy365 under this Service Guide.

1 *DETAILS OF SERVICE*

1.1 *REDSPY365^{SM}: PTAAS FLEX*

RedSpy365 monitors the IT Infrastructure utilizing cloud-based virtual servers and on-site physical servers during pre-scheduled recurring periods over the term of service. These servers scan the external infrastructure looking for new IP addresses and ports plus any potential vulnerabilities and testing the impact of those risks to the business. RedSpy365 also keeps abreast and integrates new tactics, techniques, tools, and procedures that bad actors may be now using. When a significant event trigger occurs and an alert is generated, a RedSpy365 analyst will review the alert for criticality and impact then notify one of the designated CUSTOMER Points of Contact (POC) to discuss remediation and/or further potential exploitation. All monitoring policies will be configured to send email alerts to both RedSpy365 personnel and the appropriate CUSTOMER POC to ensure that all appropriate parties receive immediate notification that a significant event has occurred.

- The target IP addresses/FQDN's will be scanned and tested automatically with manual review and post-exploitation. These addresses will be provided by the CUSTOMER. Any changes to the address range should be reported immediately to RedSpy365.
- Vulnerability scans will be determined by the base flex module purchased (monthly or quarterly) The timing can be determined by the CUSTOMER. The scanning IP address should be whitelisted in security devices that will interfere with the results of the scan.

Standard Operating Procedures (SOP) are executed when an alert is triggered. The protocol that will be followed when an alert is triggered is as follows:

1. A new IP/port/vulnerability/TTP detected.
2. Alerts sent to the Redspy365 analyst/team who are monitoring the CUSTOMER portal
3. If an alert is not generated by RedSpy365, an alert will be sent via Internet Chat Channel (IRC) or another method as defined by the client.
4. RedSpy365 analysts send a response to the client detailing the IP and port with an exact level of compromise achieved/risk noted.

    1. If compromise is achieved, an initial priority precedence technical report is sent to the client.
    2. An initial flash precedence technical report, if an automated compromise is achieved, is sent to the client with a phone call to the primary contact (contained in an alert from RedSpy365).

5. Simultaneously, when the RedSpy365 Penetration Testing Team receives an alert that an initial vulnerability assessment has been completed, additional information may be sent to the client as needed. This will contain the technical data and other data to form a product report.

    1. The product report will contain risk rating and action precedence.
    2. Based on the Service Level Agreement (SLA), the client will decide how to handle compromised, critical, high, medium, or low-risk ratings.

1.2 *REDSPY365 TECHNICAL SUPPORT CENTER CONTACT INFORMATION*

Analyst Email Security_Engineer@RedSpy365.com[1]
Lead Security Analyst Number: (276) 639-9575
Individual RedTeam analyst contact details will be provided upon assignment

1.3 *REQUIREMENTS AND ASSUMPTIONS*

To ensure sustainable support to CUSTOMER, RedSpy365 requires the following to be completed prior to the initiation of this Agreement:

1. CUSTOMER must provide a single Point of Contact (POC) that has the authority to approve purchases (hardware, software, services, etc.), act as a liaison between CUSTOMER and RedSpy365 when there are billing or scope questions, and coordinate scheduling with RedSpy365 to ensure access and availability to CUSTOMER's resources.
2. CUSTOMER will provide clear vendor escalation paths and processes for their 3rd party vendors.
3. CUSTOMER agrees to provide three (3) days advanced notification of any changes to the covered devices or software including physical locations and/or network address changes.
4. CUSTOMER will provide the appropriate administrative access to systems and applications as requested by RedSpy365.

1.4 *AGREEMENT CONDITIONS*

This Agreement will remain in effect for one (1) year from the date of acceptance, which is defined as a signature from a CUSTOMER representative. At the end of the contract term, this Agreement may be renegotiated. CUSTOMER agrees to allow RedSpy365 to amend the original agreement if additional services are requested within the lifecycle of this contract. Additional costs for additional services require CUSTOMER's written approval and would be added to the following month's invoice.
Except as otherwise stated in this Agreement, changes to this Agreement (other than a termination request) must be agreed to and authorized in writing by both CUSTOMER and RedSpy365. The changes will be added to this Agreement and defined as "the addition to or change of any services originally defined in the approved, signed-off Agreement."
Either party may cancel this Agreement with or without cause prior to its completion with a thirty (30) days written notice of their intent *. Notwithstanding anything in this Agreement to the contrary, CUSTOMER may terminate this Agreement immediately if RedSpy365 fails to maintain the confidentiality of CUSTOMER information *.

*This overrides the InterVision MSA Agreement early termination item 4.2.

2 *SERVICES INCLUDED*

Services	***Flex Default***	***Optional Add ons***
Gap Analysis via SIG	***X***	

1 mailto:Security_Engineer@RedSpy365.com

Cloud Appliance for External testing	X	
On-Site Appliance for Internal testing		X
Full Development VM to develop integrations or VM		X
External Penetration Test During onboarding, the analyst initiated	X	X
External Penetration Testing – recurring	X	
Internal Penetration Test during onboarding, analyst initiated		X
Internal Penetration Testing – recurring		X
Social Engineering Training On-demand – Access to RedSpy365 knowledge base for self-paced training		X
On-demand reporting – Self-service	X	
On-demand reporting – Analyst-assisted report generation		X
Standard Web Application Testing		X
Advanced Web Application Testing		X
3rd Party Breach Alerts		X
Credential Monitoring Alerts		X
Threat Intel, Risk Mapping, and Alerting		X
Compliance and AI Mapping		X
RS Scout Advanced Malware		X
Advanced Email Phishing		X
Agger - Anti Ransomware		X

*Overrides InterVision MSA items 9.0,10.0

2.1 *DEFINITIONS:*

RedSpy365 Flex Core 4 (Quarterly)

Base RedSpy365 Core - (Cloud VM, Vuln scan, RSTooling and Market place Access)
Cloud Based Appliance for External testing
External Penetration Testing 4 Times per year
On-demand reporting – Self-service
Access to support analysis via email/ticket – business hours
Access to Market Place
Analyst Tools and Tool Access Portal
Host and web Vulnerability Scans (Recon, Enum, Exploitation and Post Exploitation)

RedSpy365 Flex Core 12 (Monthly)

Base RedSpy365 Core - (Cloud VM, Vuln scan, RSTooling and Market place Access)
Cloud Based Appliance for External testing
External Penetration Testing 12 Times per year
On-demand reporting – Self-service
Access to support analysis via email/ticket – business hours
Access to Market Place
Analyst Tools and Tool Access Portal
Host and web Vulnerability Scans (Recon, Enum, Exploitation and Post Exploitation)

RedSpy365 Flex Core+ 1 (Monthly External, One Internal)

Base RedSpy365 core + (Cloud VM, VM Onsite, Vuln scan, RS Tooling and Market place Access)
Cloud Based Appliance for External testing + Free VM for internal testing
External Penetration Testing 4 Times per year
Internal Once per year
On-demand reporting – Self-service
Access to support analysis via email/ticket – business hours
Access to Market Place
Analyst Tools and Tool Access Portal
Host and web Vulnerability Scans (Recon, Enum, Exploitation and Post Exploitation)

RedSpy365 Flex Core+ 5 (monthly External, Quarterly Internal +One)

Base RedSpy365 Core+ (Cloud, VM Onsite, Vuln scan, RS Tooling and Market place Access)
Cloud Based Appliance for External testing + Free VM for internal testing
External Penetration Testing 12 Times per year
Internal 5 times per year
On-demand reporting – Self-service
Access to support analysis via email/ticket – business hours
Access to Market Place
Analyst Tools and Tool Access Portal
Host and web Vulnerability Scans (Recon, Enum, Exploitation and Post Exploitation)

Standard Web application testing:

For more basic web applications. Web application testing using a combination of tools and human effort. This can be run weekly and/or on demand.

Advanced Web application testing:

For more complicated websites and credentialed testing scans. Advanced web application testing using state-of-the-art web application scanning tools and human effort. Designed to be false positive free. This can be run weekly and/or on demand. This type of testing goes beyond basic functionality checks and aims to identify more complex issues that might impact the application's performance, security, and user experience.

3rd Party Breach Alerts

- Locating compromised credentials from sources unique to our research capability, including human, machine, and malware sources
- Early identification enables organizations to respond quickly and prevent or nullify possible damage
- Monitoring capabilities for your employees, customers, and VIP personnel to mitigate credential exposure
- Advising organizations on lockouts and account resets for quick protection against compromised credentials

Intel 471 Credential Monitoring Continuous

- Locating compromised credentials from sources unique to our research capability, including human, machine, and malware sources
- Early identification enables organizations to respond quickly and prevent or nullify possible damage
- Monitoring capabilities for your employees, customers, and VIP personnel to mitigate credential exposure
- Advising organizations on lockouts and account resets for quick protection against compromised credentials

SIG Compliance and AI Mapping

Often a technical failure is the symptom of control object and compliance failure. Understanding and mapping risk to compliance enable an organization to move away from remediating just technical issues, but now to identify control objects and compliance failures. Obviously, nobody enjoys filling out compliance questions, but our secure AI can search and automatically fill out compliance questions based on your own policies and procedures. RedSpy365 can help map control object failures, often root causes of technical issues, to almost any compliance requirement. This creates a separate report that a client can download. In completing a SIG with the help of AI, when a significant risk occurs the client can understand what control object/objects failed to allow that significant risk to occur. RedSpy can help identify systemic control object failures that will need to be addressed to help prevent future technical failures.

RS Scout Advanced Malware

The most advanced malware implant on the planet. Designed out of the box to avoid modern AV/EDR and security defenses it is continuously updated and tests systems using advanced tactics and techniques that only advanced bad actors and nation-states would use. Take your testing to the next level.

Advanced Email Phishing

Phishing testing, also known as phishing simulation or phishing awareness testing, is a proactive approach to assessing and improving an organization's cybersecurity defenses against phishing attacks. It involves conducting controlled and simulated phishing attacks on employees to evaluate their susceptibility to falling for phishing scams. The primary goal of phishing testing is to identify vulnerabilities and areas of weakness within an

organization's workforce and security infrastructure.
Using advanced cloaking and other techniques, email phishing is often the attack vector of most bad actors. With templates and landing pages updated all the time, email phishing can be malware delivery credential stealing, or any other form of data stealing, or manipulation. This can be continuously run, or run as campaigns we approved phishing templates and landing pages.

Internal Appliance

For internal penetration testing if the client cannot use a VM we can provide an appliance to run the VM on.

Agger - Anti Ransomware

Anti-Ransomware Anti-Wiperware Software

NOTE: Support services onboarding takes up to Three business weeks to complete. The onboarding process is dependent on CUSTOMER cooperation and willingness to address their respective onboarding actions in a timely manner.