PTAAS POWERED BY REDSPY 365 - SERVICE GUIDE

Last Modification Date: 12/07/2023
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}: A CONTINUOUS PENETRATION TESTING SERVICE*

RedSpy365 monitors the IT Infrastructure utilizing cloud-based virtual servers and on-site physical servers 24 hours a day over the term of service. These servers scan the external infrastructure looking for new IP addresses and ports plus any potential vulnerabilities. When an event trigger occurs and an alert email 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. 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 an event has occurred.

- The target IP addresses will be scanned and tested automatically. These addresses will be provided by the CUSTOMER. Any changes to the address range should be reported immediately to RedSpy365.
- Vulnerability scans will be conducted as needed The timeframe can be determined by the CUSTOMER, but RedSpy365 recommends a minimum of once a week. 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 detected via Virtual Pen Tester™.
2. Virtual Pen Tester™ sends emails to the Redspy365 analyst/team who are monitoring the CUSTOMER portal
3. If an email alert is not generated by Virtual Pen Tester™, 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 via attack botnet.

1. If no automated 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 email from Virtual Pen Tester™).

5. Simultaneously, when the RedSpy365 Penetration Testing Team receives an email 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.

We may include a 24/7 response for a compromised action and a portal for clients depending upon SLA required.

1.2 *EMAIL PHISHING, TRAINING, AND TESTING*

RedSpy365 sends emails to designated addresses at designated times. The emails sent will be registered in a report that is emailed once a week to the designated CUSTOMER POC. Emails that are clicked upon will be redirected to training CUSTOMER and/or run exploit modules. Training CUSTOMERs will register when the user has completed the training by having the user click on a pop-up after the training CUSTOMER has been viewed. Exploit emails will contain PDF attachments and/or Java pop-ups. If a user clicks on the Java pop-up, the system will attempt an attack. This will trigger the notification procedure as described in Section A. An email will be sent once a week

containing a report outlining user profiles. The client portal will be configured to send notifications of any compromise to RedSpy365 analysts and <CUSTOMER POC.

- Email campaigns will be sent based on email addresses provided by the CUSTOMER.
- The percentage of training emails to exploit emails will be decided by the CUSTOMER.

Standard Operating Procedures (SOPs) are executed when a training email is clicked. The training email SOP runs as follows:
1. Training email clicked.
2. Click is registered.
3. If the training pop-up was completed, the date and time of training completion are noted.
4. A report is sent once a week showing the number of emails clicked, the amount redirected, and if the training was completed.
Standard Operating Procedures (SOPs) are executed when an exploit email is clicked. The exploit email SOP runs as follows:
1. Exploit email clicked and exploit run.
2. Virtual Pen Tester™ sends emails to RedSpy365 Analysts/team who are monitoring the CUSTOMER portal.
3. If an email alert is not generated by Virtual Pen Tester™, an alert will be sent via Internet Chat Channel (IRC) or another method as defined by the client.
4. RedSpy365 Analyst/team sends template response to the client detailing IP and port findings plus the exact type of compromise achieved via attack botnet.

- An initial priority precedence technical report, if no automated compromise is achieved, is sent to the client.
- 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 email from a pen test virtual machine.)

5. Simultaneously, when the RedSpy365 Penetration Testing Team receives an email 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.

- The product report will contain risk rating and action precedence.
- Based on the SLA, CUSTOMER will decide how to handle compromised information based on high, medium, or low-risk ratings.

1.3 *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

1.4 *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.

1 mailto:Security_Engineer@RedSpy365.com

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.

1.5 *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	*Core*	*Core +*
Email Phishing, Training, and Testing	*X*	*X*
Gap Analysis via SIG	*X*	*X*
Cloud Based Appliance for External testing	*X*	*X*
On-Site Appliance for Internal testing		*X*
Full Development VM to develop integrations or VM		*X*
External Penetration Test during onboarding, analyst initiated	*X*	*X*
External Penetration Testing – Continuous	*X*	*X*
Internal Penetration Test during onboarding, analyst initiated		*X*
Internal Penetration Testing – Continuous		*X*

Social Engineering Training On-demand – Access to RedSpy365 knowledge base for self-paced training	X	X
On-demand reporting – Self-service	X	X
On-demand reporting – Analyst-assisted report generation		X
Basic Web Application Testing	X	X
Advanced Web Application Testing (includes 5 FQDNs)		X
Access to support analysis via email/ticket – business hours with 8-hour response SLA	X	X
Access to support analysis via Phone/live chat – business hours with 4-hour response SLA*		X

*Overrides InterVision MSA items 9.0,10.0

2.1 *DEFINITIONS:*

Basic web application testing:

Using manual, open-source tooling and automated targets the top 10 OWASP risks

Advanced web application testing:

Using manual, open source tooling and advanced testing false positive free intensive web application testing. Can map to multiple web compliance regulations.

3rd Party Breach Notification includes the following additional services:

- 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

Credential Monitoring includes the following additional services:

- Locating compromised credentials from sources unique to our research capability, including human, machine, and malware sources
- Early identification that 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

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.