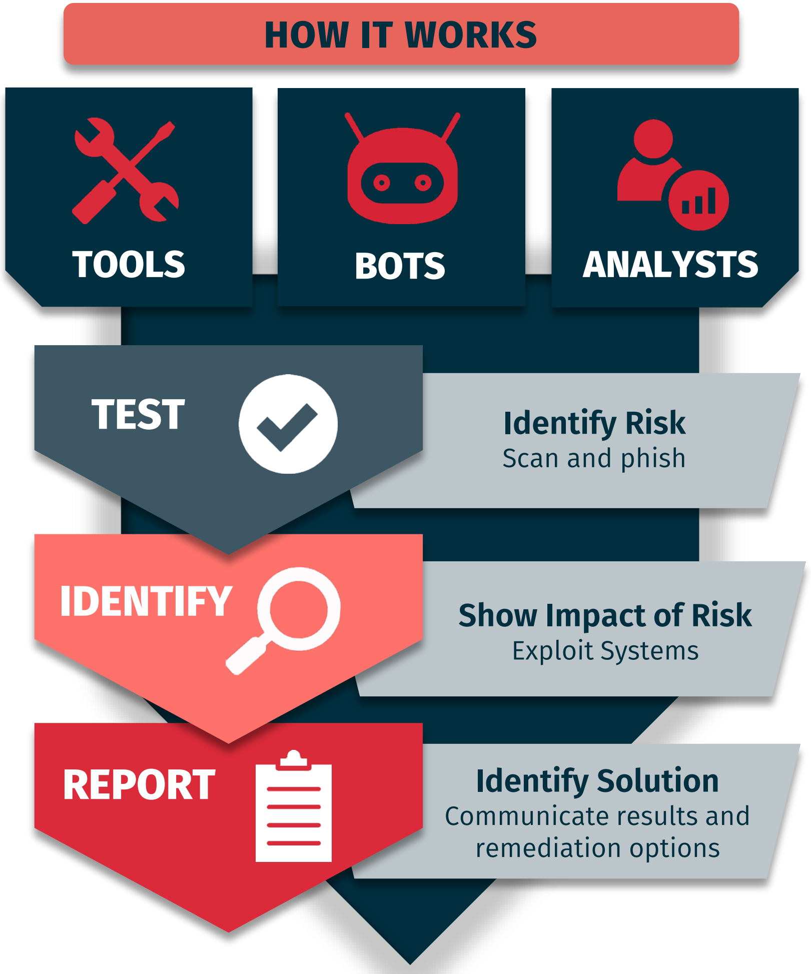
RedSpy^{365}™

Continuous Penetration Testing as a Service

What is RedSpy^{365}?



- RedSpy^{365} is the only live, un-simulated, PTaaS* and attack-modeling platform that is able to mimic the potential effects of specific hacker groups and calculate real business impacts.
- Developed by Darren Manners, one of a limited number of Blue and Red SANS Cyber Guardians in the world.
- RedSpy^{365} validates your security infrastructure and provides greater detail and actionable insight than *any other cybersecurity tool on the market today.*
- It combines over 200 security tools and allows them to talk to one another and share information using a proprietary system of variables and bots.

*Penetration Testing as a Service.

Benefits of RedSpy^{365}

- Instantly save money with our real-time reports instead of your scheduled penetration tests.
- Gain peace of mind from a service that constantly tests your defenses and alerts to concerns.
- Increase your resilience with complete phishing testing and security awareness training.
- Stay cyber compliant as regulations change.
- Manage enterprise risk with market-leading metrics.
- Maximize the value of your defensive investments by comparing our offensive testing log to your SIEM.
- Save time with dynamic troubleshooting insights and easy retesting.

Business Value

$485,000+

RedSpy^{365} Core	$35,000
RedSpy^{365} Core+	$65,000
RedSpy^{365} Enterprise	As Scoped
Benefits	
Weekly reports + 4-8-hour SLA Support	$30,000
24/7/365 Proactive Attack Modeling	$100,000
Quarterly Penetration Tests	$60,000
Industry-leading Risk Management	$250,000
Access to Best-in-Breed Tools	$15,000
Proactive Compliance Guidance	$30,000
VALUE	**$485,000**

Typical 6-Month Results

- A reduction in mean dwell time (MDT) from the industry average of over 200 days to less than one week.
- Substantial avoidance of potential economic loss, from tens of thousands to tens of millions.
- Key business continuity insights that prioritize security focus.
- Increased compliance factors to nearly 100%.
- A return on security investment (ROSI) of well over 300%.

Who Uses RedSpy365?

- Banks and Credit Unions
- Insurance Companies
- Health Systems
- Pharmaceutical Firms
- SaaS Providers
- Hospitality
- Retail
- Colleges and Universities
- Cities and Municipalities
- Manufacturing Firms
- 3PL Firms
- Wealth Management Firms
- Consultancies
- M&A Firms

References available upon request in your industry.

How does RedSpy365 Manage Cyber Risk?

Cyber Risks:

Stay safe from hackers, ransomware, or loss of PII. RedSpy365 gets beyond surface risk to root causes so you can resolve key issues for good.

Operational Risks:

Map likely attack paths to critical business processes via our asset inventory. Stay up and running.

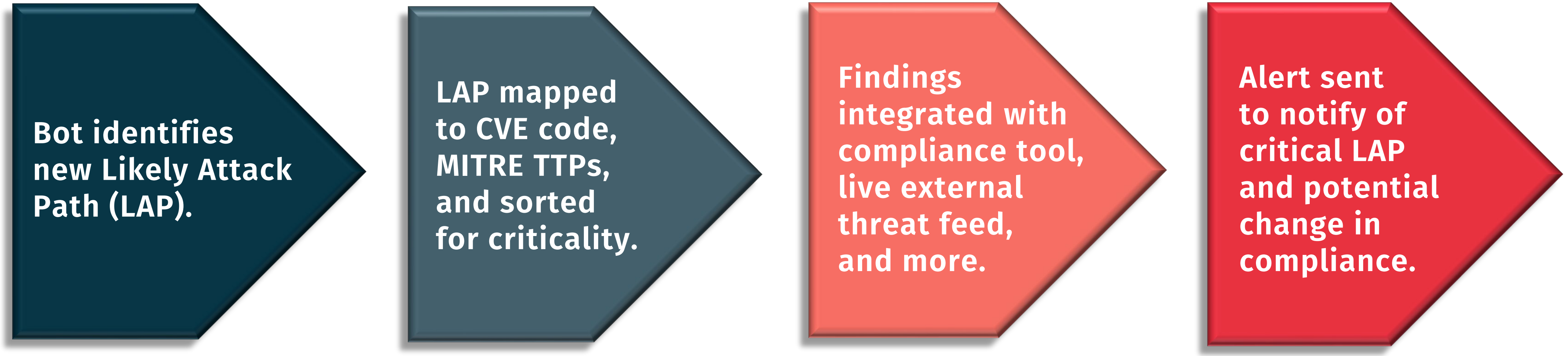
Economic Risks:

Map likely attack paths to Single Loss Expectancy (SLE), a measure of avoided economic loss. We use this, and other metrics, to calculate the ROI of using RedSpy365.

Compliance Risks:

Use the SIG Core Integration to ensure cyber compliance for your industry.

Using Bots to Model Attacks



Bot identifies new Likely Attack Path (LAP).

LAP mapped to CVE code, MITRE TTPs, and sorted for criticality.

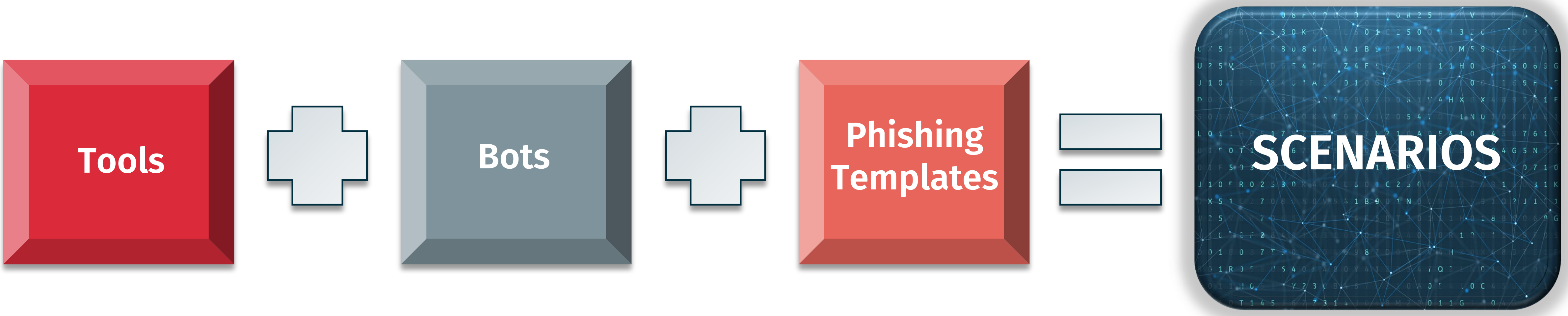
Findings integrated with compliance tool, live external threat feed, and more.

Alert sent to notify of critical LAP and potential change in compliance.

Bots can be programmed to ALERT for:

- Criticality
- Potential economic impact
- Compliance risk
- Impact on business processes
- Relevance to external threats
- Gaps in detection systems

Creating a RedSpy365 Scenario to Model Complex Threats

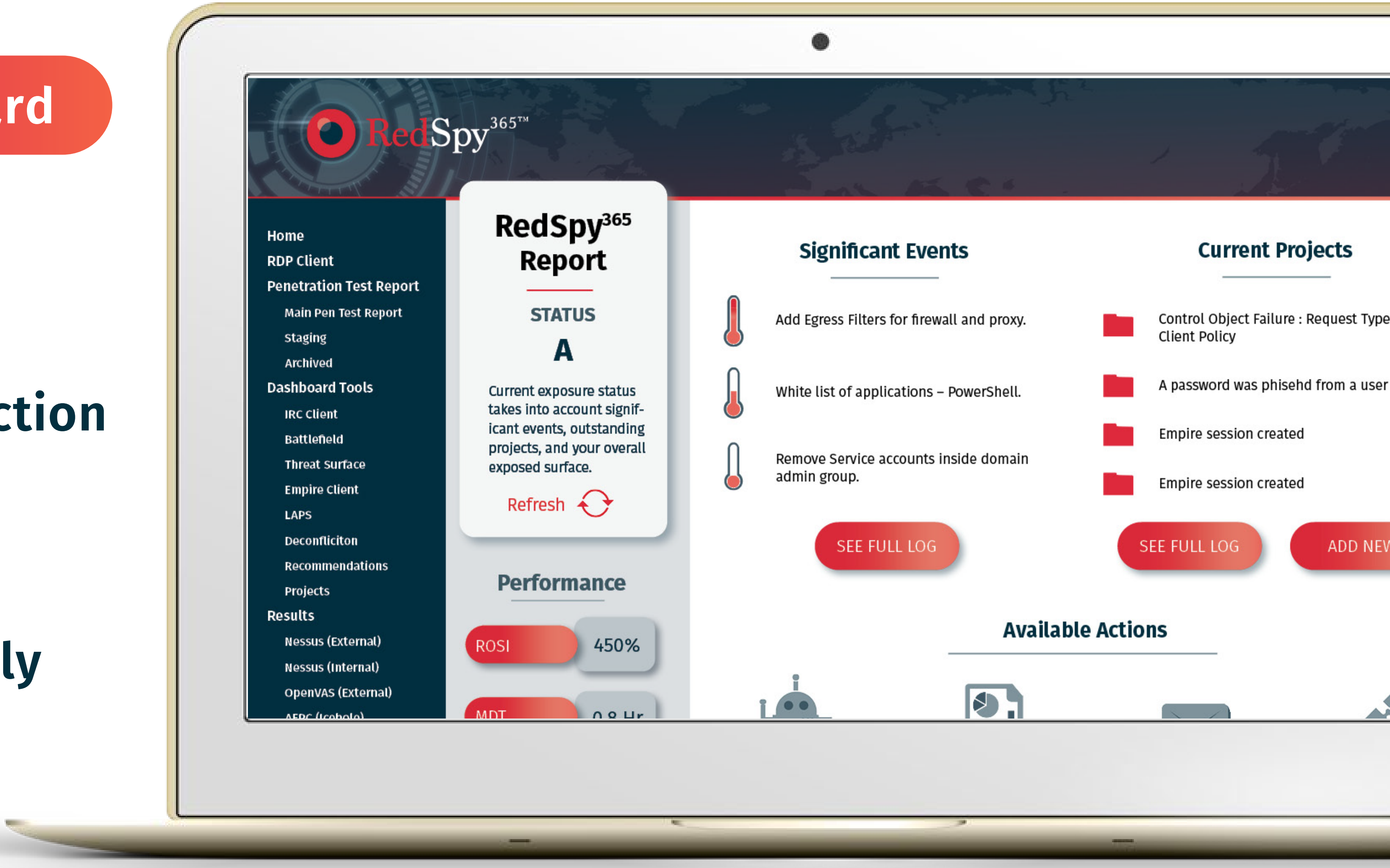


Sophisticated, complex scenarios can be built using the Scenario Builder. Users can run complicated threat models in their live environment.

Security consultants and enterprises can store scenarios in a private library and run the model when desired against all clients or installations at one time.

Convenient Dashboard

- View your status
- Print reports
- Investigate + take action
- Resolve + retest
- Prioritize resources
- Access tools remotely



RedSpy365 Report

STATUS

A

Current exposure status takes into account significant events, outstanding projects, and your overall exposed surface.

Performance

ROSI	450%
MDT	0.8 Hr

Significant Events

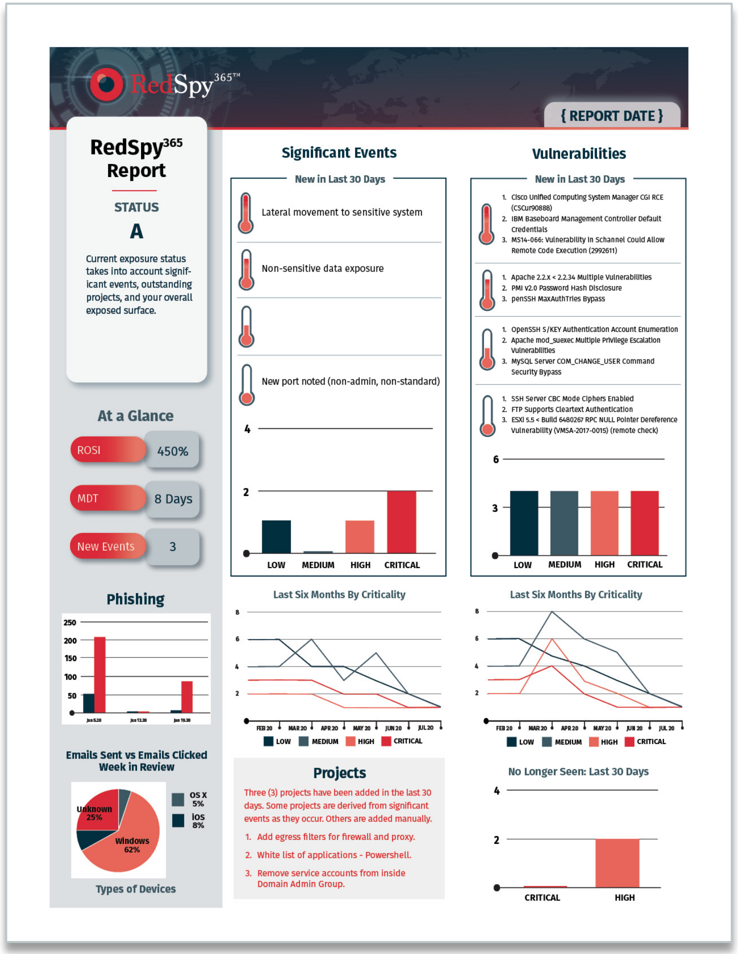
- Add Egress Filters for firewall and proxy.
- White list of applications – PowerShell.
- Remove Service accounts inside domain admin group.

Current Projects

- Control Object Failure : Request Type Client Policy
- A password was phisehd from a user
- Empire session created
- Empire session created

Available Actions

Flexible, Dynamic Reporting Options



RedSpy365™

{ REPORT DATE }

RedSpy365 Report

STATUS

A

Current exposure status takes into account significant events, outstanding projects, and your overall exposed surface.

At a Glance

ROSI	450%
MDT	8 Days
New Events	3

Phishing

Emails Sent vs Emails Clicked Week in Review

Types of Devices

Significant Events

New in Last 30 Days

- Lateral movement to sensitive system
- Non-sensitive data exposure
- New port noted (non-admin, non-standard)

Last Six Months By Criticality

Projects

Three (3) projects have been added in the last 30 days. Some projects are derived from significant events as they occur. Others are added manually.

1. Add egress filters for firewall and proxy.
2. White list of applications - Powershell.
3. Remove service accounts from inside Domain Admin Group.

Vulnerabilities

New in Last 30 Days

1. Cisco Unified Computing System Manager CGI RCE (CSCur90888)
2. IBM Baseboard Management Controller Default Credentials
3. MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)

1. Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
2. PMI v2.0 Password Hash Disclosure
3. penSSH MaxAuthTries Bypass

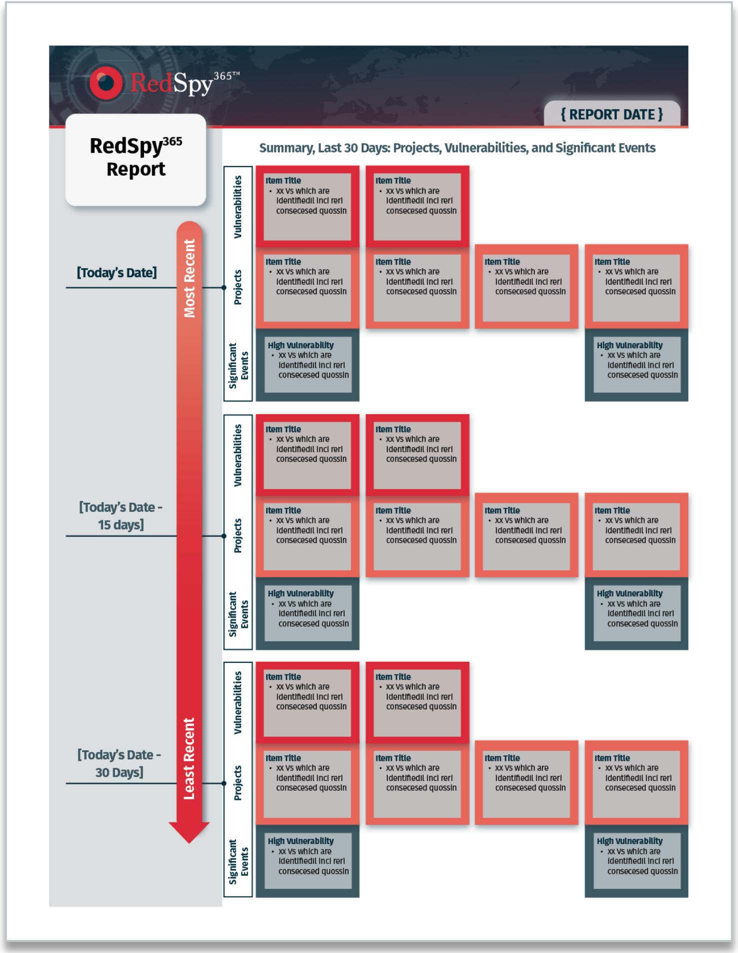
1. OpenSSH S/KEY Authentication Account Enumeration
2. Apache mod_suexec Multiple Privilege Escalation Vulnerabilities
3. MySQL Server COM_CHANGE_USER Command Security Bypass

1. SSH Server CBC Mode Ciphers Enabled
2. FTP Supports Cleartext Authentication
3. ESXi 5.5 < Build 6480267 RPC NULL Pointer Dereference Vulnerability (VMSA-2017-0015) (remote check)

Last Six Months By Criticality

No Longer Seen: Last 30 Days

- Summary 30-day report
- PCISS-compliant pen tests
- Proactive + reactive
- Compliance alerts
- Phishing test results
- Open projects
- 3-, 6-, 9-month trends



RedSpy365™

{ REPORT DATE }

RedSpy365 Report

Summary, Last 30 Days: Projects, Vulnerabilities, and Significant Events

[Today's Date]

Vulnerabilities

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Projects

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Significant Events

High Vulnerability
- xx Vs which are identifiedil inci reri consecesed quossin

High Vulnerability
- xx Vs which are identifiedil inci reri consecesed quossin

[Today's Date - 15 days]

Vulnerabilities

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Projects

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Significant Events

High Vulnerability
- xx Vs which are identifiedil inci reri consecesed quossin

High Vulnerability
- xx Vs which are identifiedil inci reri consecesed quossin

[Today's Date - 30 Days]

Vulnerabilities

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Projects

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

Item Title
- xx Vs which are identifiedil inci reri consecesed quossin

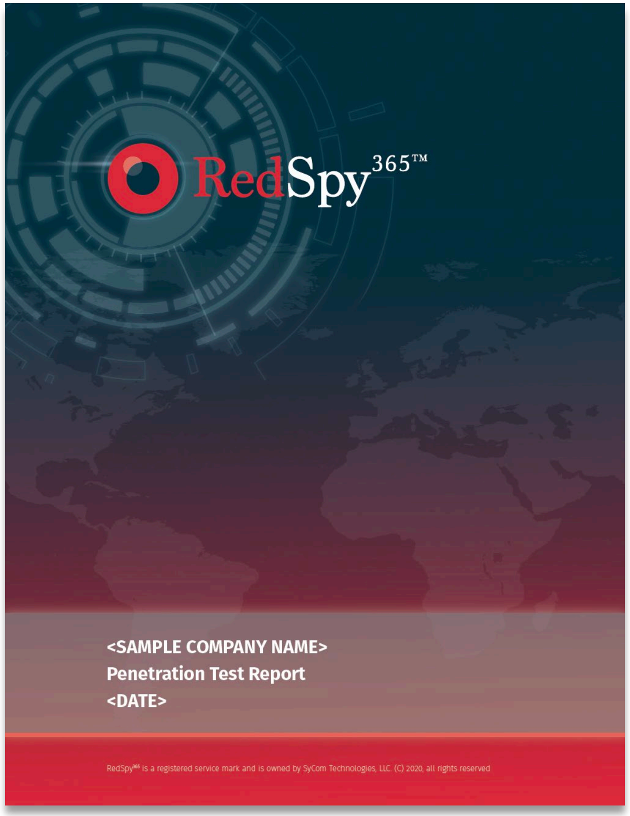
Significant Events

High Vulnerability
- xx Vs which are identifiedil inci reri consecesed quossin

High Vulnerability
- xx Vs which are identifiedil inci reri consecesed quossin

Auditor-Ready Penetration Test

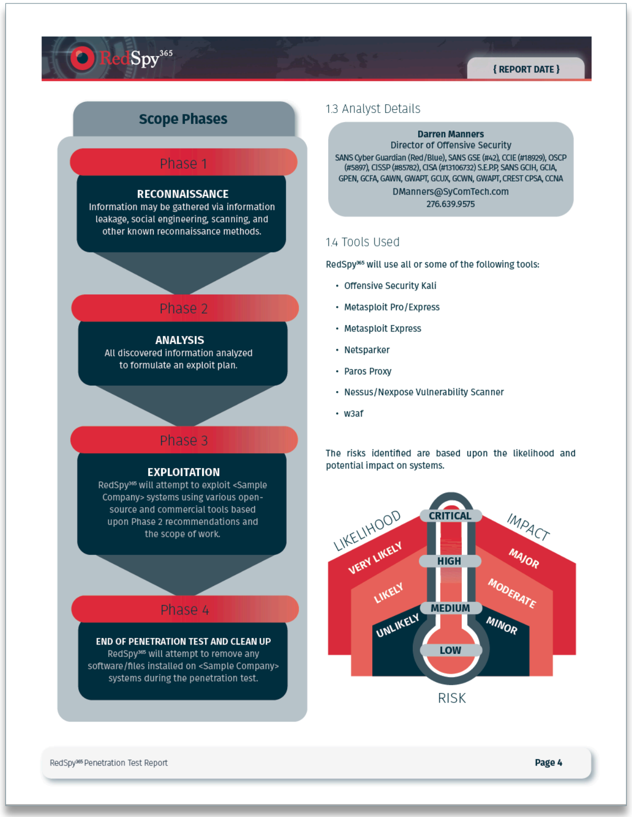
RedSpy^{365} produces PCISS-compliant penetration tests on demand.



RedSpy$^{365™}$

<SAMPLE COMPANY NAME>
Penetration Test Report
<DATE>

RedSpy^{365} is a registered service mark and is owned by SyCom Technologies, LLC. (C) 2020, all rights reserved



RedSpy^{365} { REPORT DATE }

Scope Phases

Phase 1

RECONNAISSANCE
Information may be gathered via information leakage, social engineering, scanning, and other known reconnaissance methods.

Phase 2

ANALYSIS
All discovered information analyzed to formulate an exploit plan.

Phase 3

EXPLOITATION
RedSpy^{365} will attempt to exploit <Sample Company> systems using various open-source and commercial tools based upon Phase 2 recommendations and the scope of work.

Phase 4

END OF PENETRATION TEST AND CLEAN UP
RedSpy^{365} will attempt to remove any software/files installed on <Sample Company> systems during the penetration test.

1.3 Analyst Details

Darren Manners
Director of Offensive Security
SANS Cyber Guardian (Red/Blue), SANS GSE (#42), CCIE (#18929), OSCP (#5897), CISSP (#85782), CISA (#13106732) S.E.P.P, SANS GCIH, GCIA, GPEN, GCFA, GAWN, GWAPT, GCUX, GCWN, GWAPT, CREST CPSA, CCNA
DManners@SyComTech.com
276.639.9575

1.4 Tools Used

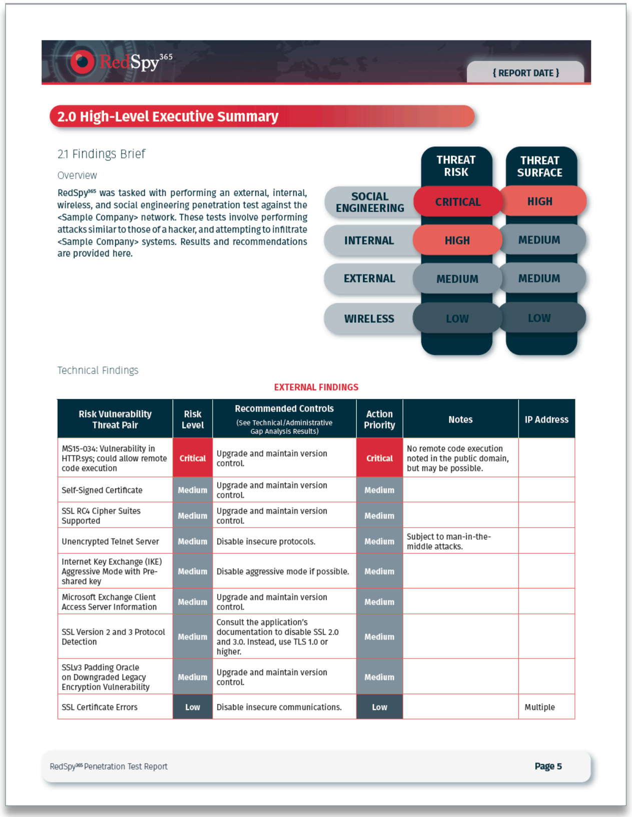
RedSpy^{365} will use all or some of the following tools:

- Offensive Security Kali
- Metasploit Pro/Express
- Metasploit Express
- Netsparker
- Paros Proxy
- Nessus/Nexpose Vulnerability Scanner
- w3af

The risks identified are based upon the likelihood and potential impact on systems.

LIKELIHOOD
VERY LIKELY
LIKELY
UNLIKELY
CRITICAL
HIGH
MEDIUM
LOW
IMPACT
MAJOR
MODERATE
MINOR
RISK

RedSpy^{365} Penetration Test Report   Page 4



RedSpy^{365} { REPORT DATE }

2.0 High-Level Executive Summary

2.1 Findings Brief

Overview

RedSpy^{365} was tasked with performing an external, internal, wireless, and social engineering penetration test against the <Sample Company> network. These tests involve performing attacks similar to those of a hacker, and attempting to infiltrate <Sample Company> systems. Results and recommendations are provided here.

	THREAT RISK	THREAT SURFACE
SOCIAL ENGINEERING	CRITICAL	HIGH
INTERNAL	HIGH	MEDIUM
EXTERNAL	MEDIUM	MEDIUM
WIRELESS	LOW	LOW

Technical Findings

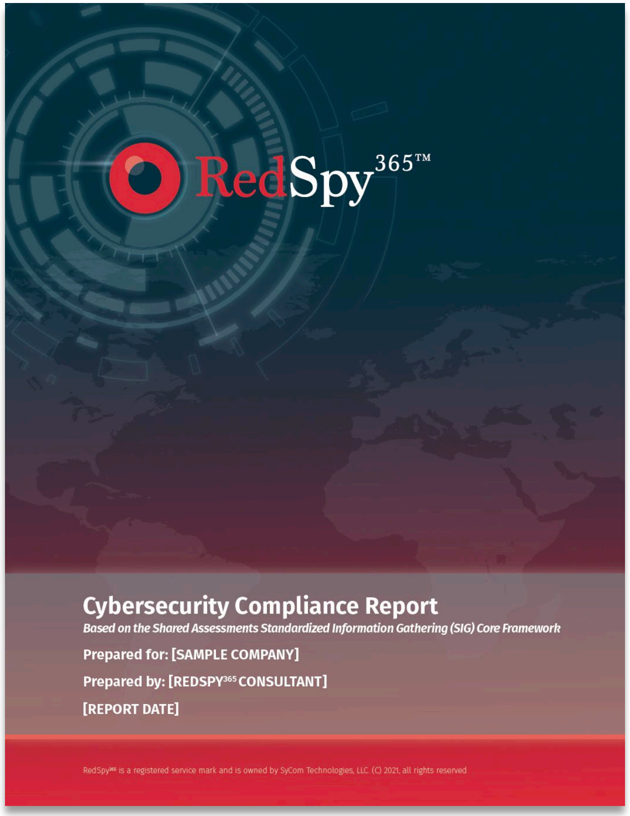
EXTERNAL FINDINGS

Risk Vulnerability Threat Pair	Risk Level	Recommended Controls (See Technical/Administrative Gap Analysis Results)	Action Priority	Notes	IP Address
MS15-034: Vulnerability in HTTP.sys; could allow remote code execution	Critical	Upgrade and maintain version control.	Critical	No remote code execution noted in the public domain, but may be possible.	
Self-Signed Certificate	Medium	Upgrade and maintain version control.	Medium		
SSL RC4 Cipher Suites Supported	Medium	Upgrade and maintain version control.	Medium		
Unencrypted Telnet Server	Medium	Disable insecure protocols.	Medium	Subject to man-in-the-middle attacks.	
Internet Key Exchange (IKE) Aggressive Mode with Pre-shared key	Medium	Disable aggressive mode if possible.	Medium		
Microsoft Exchange Client Access Server Information	Medium	Upgrade and maintain version control.	Medium		
SSL Version 2 and 3 Protocol Detection	Medium	Consult the application's documentation to disable SSL 2.0 and 3.0. Instead, use TLS 1.0 or higher.	Medium		
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability	Medium	Upgrade and maintain version control.	Medium		
SSL Certificate Errors	Low	Disable insecure communications.	Low		Multiple

RedSpy^{365} Penetration Test Report   Page 5

Compliance Report

RedSpy^{365} integrates with the Shared Assessments compliance tool to report on cyber security readiness and guide your next steps.



RedSpy$^{365™}$

Cybersecurity Compliance Report

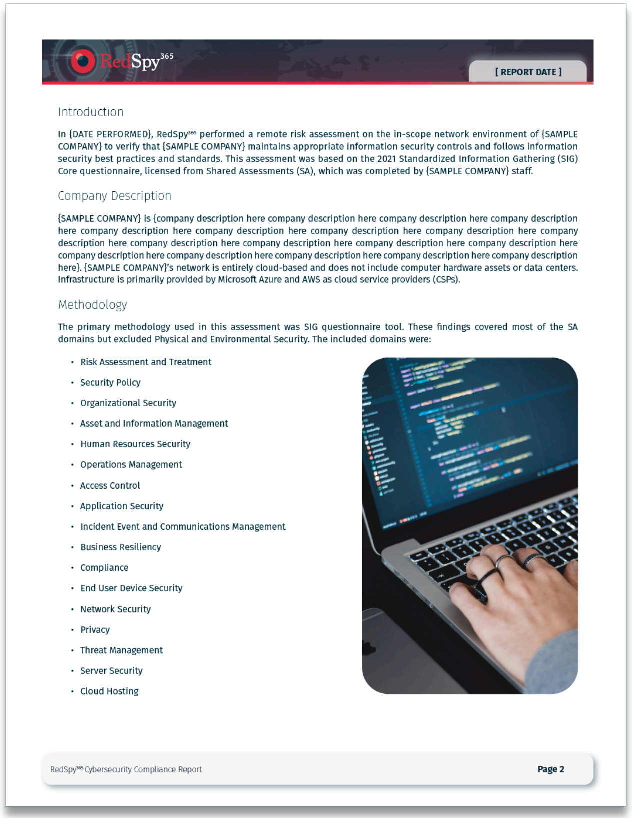
Based on the Shared Assessments Standardized Information Gathering (SIG) Core Framework

Prepared for: [SAMPLE COMPANY]

Prepared by: [REDSPY^{365} CONSULTANT]

[REPORT DATE]

RedSpy^{365} is a registered service mark and is owned by SyCom Technologies, LLC. (C) 2021, all rights reserved



RedSpy^{365} [REPORT DATE]

Introduction

In {DATE PERFORMED}, RedSpy^{365} performed a remote risk assessment on the in-scope network environment of {SAMPLE COMPANY} to verify that {SAMPLE COMPANY} maintains appropriate information security controls and follows information security best practices and standards. This assessment was based on the 2021 Standardized Information Gathering (SIG) Core questionnaire, licensed from Shared Assessments (SA), which was completed by {SAMPLE COMPANY} staff.

Company Description

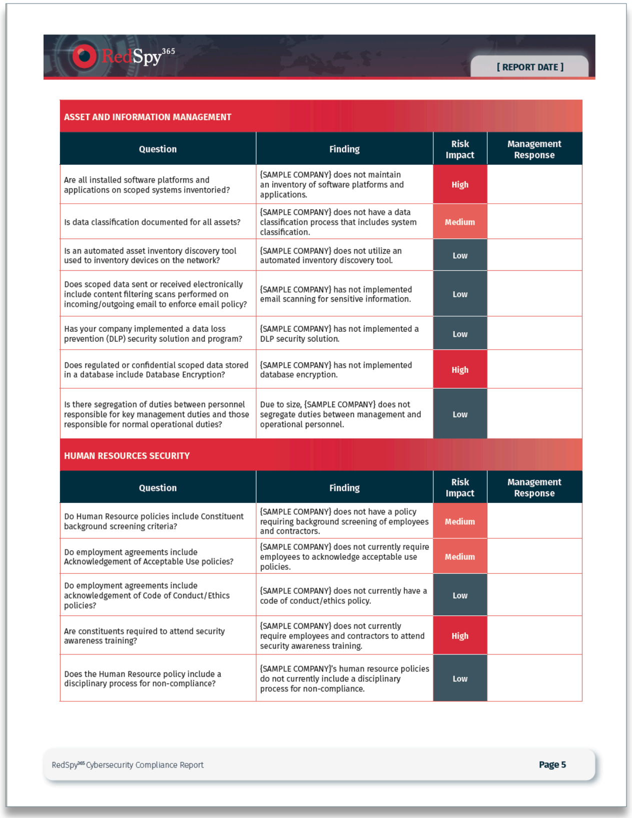
{SAMPLE COMPANY} is {company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here company description here}. {SAMPLE COMPANY}'s network is entirely cloud-based and does not include computer hardware assets or data centers. Infrastructure is primarily provided by Microsoft Azure and AWS as cloud service providers (CSPs).

Methodology

The primary methodology used in this assessment was SIG questionnaire tool. These findings covered most of the SA domains but excluded Physical and Environmental Security. The included domains were:

- Risk Assessment and Treatment
- Security Policy
- Organizational Security
- Asset and Information Management
- Human Resources Security
- Operations Management
- Access Control
- Application Security
- Incident Event and Communications Management
- Business Resiliency
- Compliance
- End User Device Security
- Network Security
- Privacy
- Threat Management
- Server Security
- Cloud Hosting

RedSpy^{365} Cybersecurity Compliance Report **Page 2**



RedSpy^{365} [REPORT DATE]

ASSET AND INFORMATION MANAGEMENT

Question	Finding	Risk Impact	Management Response
Are all installed software platforms and applications on scoped systems inventoried?	{SAMPLE COMPANY} does not maintain an inventory of software platforms and applications.	High	
Is data classification documented for all assets?	{SAMPLE COMPANY} does not have a data classification process that includes system classification.	Medium	
Is an automated asset inventory discovery tool used to inventory devices on the network?	{SAMPLE COMPANY} does not utilize an automated inventory discovery tool.	Low	
Does scoped data sent or received electronically include content filtering scans performed on incoming/outgoing email to enforce email policy?	{SAMPLE COMPANY} has not implemented email scanning for sensitive information.	Low	
Has your company implemented a data loss prevention (DLP) security solution and program?	{SAMPLE COMPANY} has not implemented a DLP security solution.	Low	
Does regulated or confidential scoped data stored in a database include Database Encryption?	{SAMPLE COMPANY} has not implemented database encryption.	High	
Is there segregation of duties between personnel responsible for key management duties and those responsible for normal operational duties?	Due to size, {SAMPLE COMPANY} does not segregate duties between management and operational personnel.	Low	

HUMAN RESOURCES SECURITY

Question	Finding	Risk Impact	Management Response
Do Human Resource policies include Constituent background screening criteria?	{SAMPLE COMPANY} does not have a policy requiring background screening of employees and contractors.	Medium	
Do employment agreements include Acknowledgement of Acceptable Use policies?	{SAMPLE COMPANY} does not currently require employees to acknowledge acceptable use policies.	Medium	
Do employment agreements include acknowledgement of Code of Conduct/Ethics policies?	{SAMPLE COMPANY} does not currently have a code of conduct/ethics policy.	Low	
Are constituents required to attend security awareness training?	{SAMPLE COMPANY} does not currently require employees and contractors to attend security awareness training.	High	
Does the Human Resource policy include a disciplinary process for non-compliance?	{SAMPLE COMPANY}'s human resource policies do not currently include a disciplinary process for non-compliance.	Low	

RedSpy^{365} Cybersecurity Compliance Report **Page 5**

RedSpy$^{365™}$

For business inquiries:

Tom Cricchi
TCricchi@SyComTech.com
804.474.5269

For a demo and/or test server credentials:

Darren Manners
DManners@SyComTech.com
276.639.9575