THE BUG STOPS HERE.

CYBER RETALIATOR SOLUTIONS

2025

ABOUT US

WHO ARE WE?

Cyber Retaliator Solutions is an Authorized IBM, RedHat, SUSE, Agile and CompTIA Training Delivery Partner and Cyber Security Distributor, Operating throughout the Globe.

Our Head Office is based in Centurion South Africa, with Training Centers in Centurion, Midrand, Sandton and Cape Town.

Cyber Retaliator Solutions is a Value Added Distributor with 20+ years of experience in Cyber Security.

TECHNICAL TRAINING CENTRE

CRS delivers Technical Training to Industry Experts Across the Globe.

Stay aligned with your customers, or internal technology through IBM Technical Training with world class trainers.

RedHat Learning helps customers stay on top of industry trends by teaching innovative technologies and products to give a competitive edge.

SUSE Technical Product Training Courses are offered via CRS. Choose a course from one of our many learning paths.

Our programme provides resources for recruiting, training, certifying and upgrading the skills of students in CompTIA.

CYBER SECURITY DISTRIBUTION

We are a future-focused business focused on bringing solutions to the African region that addresses gaps within the reselling, managed services and system integration spaces for Cyber Security.

Cyber Retaliator Solutions brings World-Class Solutions tailored to address Key Industry Challenges.

Cyber Retaliator offers Vulnerability and Penetration Testing Services to provide third party assessments through the channel.

CRS
CYBER RETALIATOR SOLUTIONS

CYBER SECURITY RANGE

VECTRA®

aikido

strobes™

SMBsecure™

Standss

BEACHHEAD®

vRx

telivy

BlueFlag Security

VAPT

CYBER RISK ESSENTIALS

flare

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

LEADER IN THE 2025 GARTNER MAGIC QUADRANT FOR NETWORK DETECTION AND RESPONSE (NDR).

Data sheet

What is VECTRA?

Vectra is the leader in AI-driven threat detection and response for hybrid and multi-cloud enterprises. Vectra's patented Attack Signal Intelligence™ technology detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyberattacks.

Gartner®
Magic Quadrant

We're proud to partner with Vectra AI, named a Leader in the first-ever 2025 Gartner® Magic Quadrant™ for Network Detection and Response (NDR) — positioned highest for Ability to Execute and furthest for Completeness of Vision.

BOOK A DEMO

CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

FUTURE PROOF YOUR CYBER DEFENSE

Vectra provides the hybrid cloud building blocks to future proof your Cyber Defense as your Attack Surface expands:

- Vectra Network Detection and Response (NDR)
- Vectra Cloud Detection and Response (CDR) for AWS
- Vectra Cloud Detection and Response (CDR) for M365
- Vectra Identity Detection and Response (IDR) for Azure AD
- Vectra Recall to query, investigate, hunt for threats
- Vectra Stream for security-enriched metadata lake
- Vectra Managed Detection and Response (MDR)

WHAT IT MEANS FOR SECURITY TEAMS

Your processes and workflows are more efficient:

- Reduce SIEM costs, detection rule creation and maintenance.
- Automate analysts' manual tasks and time to investigate and respond.
- Optimize existing investments in EDR, SOAR and ITSM.
- Reduce analyst burnout with accurate detection of malicious true positives.
- Increase analyst throughput by accelerating investigation and response.
- Builds analyst expertise and skills hunting and defending against advanced attacks.

GET THE REPORT

Figure 1: Magic Quadrant for Network Detection and Response

YOUR NO-NONSENSE SECURITY PLATFORM FOR DEVS

FROM CODE TO CI TO CLOUD

Data sheet

What is Aikido?

Aikido is a developer-centric security platform that gives developers and security teams an instant overview of all code-to-cloud security issues and guides teams to fix vulnerabilities fast. Aikido supports security teams by aggressively reducing false-positives, automatic triage and risk bundling, and translating Common Vulnerabilities and Exposures (CVEs) into easy step-by-step explanations to resolve.

HOW IT WORKS

Aikido combines features from many different platforms into one. By bringing together multiple tools into a single platform, we are able to contextualise vulnerabilities, filter out false positives, and reduce noise by 95%.

BOOK A DEMO

OPEN SOURCE DEPENDENCY SCANNING (SCA)

Continuously monitors your code for known vulnerabilities, CVEs, and other risks, or generate SBOMs.

CLOUD POSTURE MANAGEMENT (CSPM)

Detects cloud infrastructure risks (misconfigurations, VMs, and container images) across major cloud providers.

STATIC CODE ANALYSIS (SAST)

Scans your source code for security risks before an issue can be merged.

SECRETS DETECTION

Checks your code for leaked and exposed API keys, passwords, certificates, encryption keys, etc.

INFRASTRUCTURE AS CODE SCANNING (IAC)

Scans Terraform, CloudFormation & Kubernetes Helm charts for misconfigurations.

CONTAINER IMAGE SCANNING

Scans your container OS for packages with security issues.

SURFACE MONITORING (DAST)

Dynamically tests your web app's front-end & APIs to find vulnerabilities through simulated attacks – including API Scanning

OPEN SOURCE LICENSE SCANNING

Dynamically tests your web app's front-end & APIs to find vulnerabilities through simulated attacks.

AI AUTOFIX FOR SAST & IAC

Fix Static Application Security Testing (SAST) & Infrastructure as Code (IaC) issues in a single click with AI-generated fixes and Aikido's AI agent.

SDLC GOVERNANCE & SECURITY

PROTECTING THE SOFTWARE SUPPLY CHAIN

Data sheet

What is BlueFlag Security?

BlueFlag Security is transforming the industry by focusing on and reducing the risks posed by overlooked identities. This paired with industry-leading code governance and posture management tools provide a comprehensive approach to SDLC security

HOW IT WORKS

BlueFlag leverages AI-driven insights and prioritizes identity security to address critical gaps left by traditional security tools, creating a unified defense against software supply chain attacks and mitigating risks across the development lifecycle.

AICPA SOC 2 Formerly SAS 70 Reports

BOOK A DEMO

CRS CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

REMOVE EXCESSIVE PERMISSIONS

BlueFlag automates the rightsizing of permissions for developer and machine identities, enforcing the principle of least privilege throughout the dev environment.

SANITIZE POOR HYGIENE

BlueFlag enforces strong identity hygiene by deactivating off-boarded users, managing personal access tokens, and restricting direct access to developer tools and repositories.

REDUCE RISKY BEHAVIOR

BlueFlag's ensures early detection and prevention of insider threats and unauthorized privileged escalation by continuously monitoring behavior patterns across the CI/CD.

IDENTITY-CENTRIC APPROACH

BlueFlag harnesses its patented AI/ML-powered Identity Intelligence framework to accelerate risk mitigation and ensure continuous compliance.

BEYOND THE CODE

BlueFlag delivers a unified, context-rich view across all SDLC attack vectors - developer identities, tools, and code - ensuring visibility without blind spots

PRIORITIZED RISK VISIBILITY

Gain critical identity insights, ranked by priority, safeguarding against unauthorized access, insider threats, and misconfigurations.

THREAT DETECTION & REMEDIATION

Turn alert fatigue into actionable intelligence quickly addressing identity threats for effective remediation.

CONTINUOUS MONITORING

Uncover misconfigurations across the developer toolchain including source code management tools, CI/CD pipelines and container registries.

AI-DRIVEN CTEM PLATFORM

Data sheet

Who is Strobes?

"From the trenches of offensive security, we built a platform that leverages the power of advanced threat research. By uniting the expertise of security researchers, we deliver next-level Continuous Threat Exposure Management solutions."

-Venu Rao (CEO)

HOW IT WORKS

Strobes seamlessly integrates Attack Surface Management (ASM), Penetration Testing as a Service (PTaaS), and Vulnerability Management (VM) into a unified solution, providing comprehensive coverage across your entire attack surface.
Strobes enable proactive risk mitigation, preventing exploitation before it can occur.

BOOK A DEMO

ATTACK SURFACE MANAGEMENT

Set up a continuous attack surface management scan by providing keywords related to your organisation. An all-encompassing solution providing unparalleled visibility across your digital footprint. Identify all your IT assets and monitor them for vulnerabilities, zero-days, and configuration weaknesses.

PENTESTING AS A SERVICE

Meet compliance requirements by conducting on-demand or recurring penetration tests with the help of expert hackers.
Pentesting as a Service (PTaaS) offers a personalised, cost-effective, and offence-driven approach to safeguarding your digital assets. With a team of seasoned experts and advanced penetration testing methodologies, Strobes PTaaS provides actionable insights to significantly improve your security posture.

RISK BASED VULNERABILITY MANAGEMENT

Prioritize vulnerabilities using 3D context, which allows you to patch vulnerabilities in your crown jewel assets faster than ever before using threat intelligence.
Strobes RBVM simplifies vulnerability management with its all-in-one platform, streamlining the process of identifying, prioritizing, and mitigating vulnerability risks across various attack vectors. Through seamless automation, integration, and comprehensive reporting, organizations can proactively enhance their cybersecurity posture.

APPLICATION SECURITY POSTURE MANAGEMENT

Reduce risk, ensure compliance, and empower secure application development with continuous threat detection and automated vulnerability management.
Empower your business with complete visibility and control over your application security posture. Eliminate blind spots, prioritise threats effectively, and streamline remediation. Stop chasing shadows and take charge today.

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

CYBER SECURITY AUDITING

Data sheet

Who is Telivy?

Telivy is the perfect solution for Security and IT MSSPs to audit cyber security attack surfaces.
Experience the industry's most comprehensive and versatile audit tool.

HOW IT WORKS

Quantify why attention to security matters to your clients using financial metrics, insurability and ROI. Change the conversation of security tools as a hard-to-justify expense to an essential investment.

AREAS OF COVERAGE

- PII & Data Identification
- M365 and Google Workspace Assessment
- Application Inventory
- Credential Analysis
- Attack Surface
- Dark Web Scan
- Asset Discovery
- Vulnerability Assessment

ASSESS GAPS FOR CLIENTS

Walk through our cyber risk questionnaires, perform scans on your clients' environments, get an inventory of assets, and learn about their vulnerabilities. Identify solutions your clients should implement to harden their security posture. Automate these assessments periodically to gain unparalleled visibility.

BENEFITS OF TELIVY

- Visibility into 5 areas of security: Network, Data, Application, Identity and Access Policies, and Awareness.
- Complete endpoint vulnerability management.
- PII and sensitive data identification and estimation of total value.
- Identify usage of risky third-party applications.
- Strength and breach analysis of browser-based passwords.
- Dark Web analysis and Microsoft 365 tenant security recommendations

BOOK A DEMO

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

Protection & Compliance Tailored for SMBs

SMBsecure™

PC + Mobile Device + Outlook Email + USB + Phishing Defence + Supply Chain Risk + Email Domain Protection + POPIA + Risk Reporting for Compliance + Cyber Warranty + Outgoing Email Protection

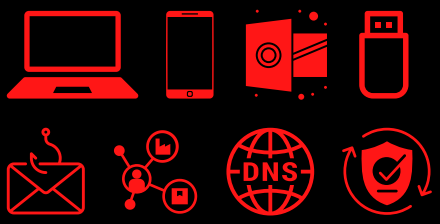
Overview of Service

SMBsecure™ is tailored to help your small business stay secure and earn trust while remaining compliant.

SMBsecure™ is an all-in-one fully managed service to de-risk your business with device & email attachment encryption, device lock & kill, phishing defence, cyber risk awareness education, reporting, and proof of data encryption & security controls.

HOW IT WORKS

SMBsecure™ leverages patented technology from leading and world class technology vendors and can be deployed in minutes to make securing your data on PCs, Mobiles and Emails a total breeze.



BOOK A DEMO

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

RISK TOOLKIT

The SMBsecure™ Risk Toolkit identifies risk in five security areas: Network, Data, Application, Identity and Access Policies, and Social Engineering susceptibility.

MISDIRECTED EMAIL AVOIDANCE

Protect from the risk of Confidential information being emailed to the wrong people. Get users to review and confirm recipients before emails are sent out.

MULTI-FACTOR AUTHENTICATION

SMBsecure™ fortifies access security on PCs and Windows Servers by verifying user logons with 2FA to stop a breach before it occurs. Secure against the use of weak, stolen, and re-used credentials (passwords) by users - a common risk - and prevent unauthorised access for any local or remote (RDP) computer logon.

CYBER AWARENESS TRAINING

SMBsecure™ offers Cyber Awareness Training and Phishing Simulations to continually enhance staff knowledge regarding cybersecurity protocols and overall awareness within organizations.

PC & MOBILE DEVICE ENCRYPTION

SMBsecure™ implements the use of data encryption on PCs and mobile devices (automatically) to secure the data on lost or stolen devices - with audit-backed proof of encryption for POPI or security validation.

PDF EMAIL ENCRYPTION

SMBsecure™ plugin for the classic Microsoft Outlook client on Windows PC provides integrated, automatic creation of password-protected Secure PDFs to secure correspondence (file attachments) with end-to-end encryption. It also includes unified FREE automatic and on-demand sending (and resending) of the password via SMS.

ACCESS CONTROL

SMBsecure™ puts safety locks in place and provides admin-initiated or automatic security measures (e.g., alerts, warnings, soft or hard lockouts, kill, and locate functions) to prevent data exposure and unauthorised access on user devices (PCs / Mobiles / USB Drives).

+ POPI Toolkit + Managed DMARC & TLS + Cyber Warranty + More

BeachheadSecure®

PROTECT YOUR PEACE OF MIND AND KEEP YOUR DATA SAFE WITH THE POWER OF ENCRYPTION ON YOUR PC, MAC, ANDROID AND IOS

Overview of Service

BeachheadSecure enables data security through native encryption and access control methods.

Encryption alone is not sufficient to protect data; it must be easily managed, enforced, and proven to be in place. BeachheadSecure offers you a managed service experience that allows for remote data access control with automated defensive features like RiskResponder to take action against recognized data risks.

WHY YOU NEED THIS

Encryption, authentication controls, password policy, location awareness, quarantine and data elimination are some of the capabilities that are at your disposal, accessed via the same, single, easy to operate policy management console managed for you that can be used to secure all your phones, PCs and Macs and USB storage devices.

BOOK A DEMO

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

COMPLETE ENCRYPTION ORCHESTRATION

With BeachheadSecure, safeguarding your data is the top priority through advanced encryption orchestration and access control functionality. By utilizing native encryption for Windows, Mac, Android, and iOS, proof of encryption is provided with a POPI Compliance Report for any lost, stolen, or compromised computer.

USB ENCRYPTION & AUTHENTICATION

BeachheadSecure offers enhanced data security features to protect sensitive data on portable USB storage devices:

- Port blocking of USB storage to prevent malicious activity.
- Mandatory encryption of confidential data on the drive.
- Option to require remote authentication to access files, with limitations on which devices can access them.
- Instant device lock and wipe capability if the storage drive is lost or stolen.

RISKRESPONDER™

With automated pre-set responses, you can ensure that you are prepared to handle a variety of situations, including invalid logon attempts, timeouts, and travel beyond geofences. RiskResponders saves you from waiting for Admin-initiated actions to secure your data.

2FA (TWO- FACTOR AUTHENTICATION)

We provide a flexible desktop multi-factor authentication solution that is reliable both online and offline. It is compatible with popular authenticator apps such as Google and Microsoft and offers an additional layer of security against unauthorized access.

POPIA COMPLIANCE REPORT

The design of BeachheadSecure supports compliance with regulations such as POPIA by allowing for reporting on device status, proof of encryption, and risk controls. The auditing system also enables tracking of changes made by administrators, ensuring device security is maintained according to specifications and any potential issues are addressed. This provides peace of mind for device monitoring and reporting on data security controls.

Beachheadsecure Plugin for Microsoft Outlook

Email Encryption | BCC ReplyGuard | Check4Phish™

Overview of Service

Prevent the unauthorised exposure of personal/sensitive data when e-mailing.

The BeachHeadSecure™ plugin for the Outlook desktop client allows for easy encryption of emails, attachments, and invitations. Secure data from sender to recipient with no files ever stored on any third-party clouds. All data remains on-device at all times. There are no requirements to make any changes to your email environment or MX records. Simply install and use it in Simple Mode or customise it for your individual requirements! It works for any email address within Microsoft Outlook on Windows PC – even Gmail!

BOOK A DEMO

HOW IT WORKS

BeachHeadSecure™ Plugin for Microsoft Outlook tightly integrates with the Outlook email client on Windows PC, providing effortless and hassle-free encryption of correspondence using the renowned **PDF** standard which means there's no keys, certificates or special decryption software needed by the recipient(s) - just a password and a PDF reader.

There's no need to generate encrypted PDFs separately - this plugin does it all for you inside Outlook - **SIMPLE!**

Securing personal data from unauthorised exposure is a critical business & compliance requirement!

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

TURNKEY WITH SIMPLE MODE

A simple out-of-box experience for the recipient and easy enough for any sender to use! Quick implementation and ready-to-go adoption guarantees an instant ROI for your business!

Simple Mode aligns to what recipients are already familiar with when receiving encrypted correspondence from their Banks which includes a password-hint to open the Secure PDF, (e.g. use ID Number).

SEND SECURELY

All password encrypted **Secure PDF** file(s) are created using **AES 256-bit** encryption prior to sending, ensuring ultra-strong security to satisfy even the strictest auditor or regulator. For extra privacy, the plugin can also automatically obscure the subject line if required.

EARN TRUST

Data Subjects want their Personal Information (PI) and sensitive data to be secured and protected, including when it is emailed. Take effective steps to safeguard recipient PI with BeachHeadSecure™.

Using this plugin to send correspondence as encrypted **Secure PDF** by email will make your business look professional. This demonstrates that you are serious about information security and handling sensitive data, to customers, stakeholders, auditors and regulators.

REMAIN COMPLIANT

The POPI Act (POPIA), other statutes, or supply chain safety require your business to provide adequate safeguards for all personal and/or sensitive data, including when it is emailed.

This plugin makes it a **total breeze for your business to safeguard personal data** when e-mailing it**.** An unencrypted **original copy** for audit and forensics is also automatically maintained inside Outlook for all encrypted email sent.

FREE PASSWORD DELIVERY BY SMS

BeachHeadSecure™ solves big challenges when using Secure PDF (*i.e. communicating the password to unlock a Secure PDF & managing all the passwords*). This plugin natively caters for embedded hint as well as automatic transmission of the **Secure PDF password** to the recipient(s), via email or by SMS at no extra costs - **the choice is yours!**

Password retrieval is made easy with ID tagging. Manage and maintain recipient passwords and preferences - **all neatly done inside Outlook!**

VULNERABILITY AND PATCH MANAGEMENT

Data sheet

What is vRx?

vRx is a comprehensive solution that combines vulnerability discovery, prioritization, and remediation into a unified platform, enhancing efficiency and security. It streamlines the process by identifying vulnerabilities, assessing their impact, and enabling effective remediation efforts through Patch Management, Auto-Actions and Patchless Protection.

HOW IT WORKS

Unleash vRx, the dynamic vulnerability and patch management solution that unveils vulnerabilities across your assets. Agents collect real-time data, powering a cloud-based hub that orchestrates a lightning-fast analysis, aligning against a vast vulnerability and patch database.
The result?
Prioritized vulnerabilities and a streamlined path to swift, precise patching and reparation – all within vRx's unified dashboard.

BOOK A DEMO

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

CONTINUOUS DETECTION OF VULNERABILITIES

You can't fix what you can't find. vRx enables 360-degree asset visibility, illuminating an exhaustive cloud-based catalogue of active servers, workstations, installed applications, and operating systems, putting you in complete control of all asset activity in real time, for both on-premise and cloud environments.

X-TAGS (CONTEXTUAL PRIORITIZATION)

Not all vulnerabilities are created equal. Focus on risks that have real potential for exploitation instead of wasting resources solving problems that don't exist. vRx prioritizes software vulnerabilities using industry-standard base metrics alongside an AI-based contextual usage risk-scoring engine, unique to your environment and priorities.

PATCH MANAGEMENT

vRx patch management fully supports Windows, macOS, and Linux. Patch vulnerabilities and deploy OS and software updates automatically and remotely. vRx is an all-in-one, lightweight agent that covers all of your vulnerability management needs. With flexible and easy-to-use tools that are managed from an intuitive interface, your IT and security teams will be able to deploy more updates faster.

AUTO-ACTIONS

vRx's Auto Actions capabilities enable your IT and cybersecurity teams to automate repetitive, tedious, and time-consuming tasks such as patch implementation so they can refocus their expertise where it's needed most. Harden your cybersecurity posture by decreasing the chance of human error and setting up automated responses to specified triggers.

PATCHLESS PROTECTION

Keep your high-risk and vulnerable apps secure even when a patch has not been developed or deployed. If flaws are published before the vendor can fix them, attackers may be able to break into systems. With vRx's Patchless Protection, vulnerable applications are shielded within a force field and secured until the next patch has been prepared, tested, and deployed.

DARK WEB MONITORING AND THREAT EXPOSURE MANAGEMENT

Data sheet

Who is Flare?

Flare was founded to empower organizations to proactively detect and remediate exposure across the clear & dark web, providing organizations with the equivalent of an automated cyber reconnaissance team.

HOW IT WORKS

Flare acts as your business's digital security bloodhound, sniffing out threats lurking on the dark web. It scans for leaked credentials, stolen data, and suspicious activity, alerting you to potential breaches before they happen. This allows you to proactively address risks and make informed security decisions to protect your company's reputation and data.

BOOK A DEMO

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

IN-DEPTH DOMAIN MONITORING

Delivers the information analysts need to positively identify and action malicious domains including screenshots, favicon updates, SSL registration, and more.

LAYERED GITHUB LEAK DETECTION

Maps relations between different assets such as commits, users, domains, and repositories for precise identification of leaks.

AUTONOMOUS TAKEDOWNS

Effortlessly action takedown requests, streamline security operations, and reduce risk in a cost-effective model.

ROBUST INTEGRATIONS

Easily integrate with SIEM, SOAR, and ticketing systems for alignment with existing security workftows.

SIMPLE LICENSING

Unlimited users, full API access, and straightforward product options to suit business needs and minimize confusion.

USE CASES

- Safeguard sensitive data
- Maintain compliance
- Protect your developers
- Rapidly detect PHI leaks
- Map your external attack surface
- Monitor the dark web for threats
- Understand the Attack Surface
- Effective Prioritization and remediation of Security breaches
- Proactive Monitoring for effective identification of risks

GOVERNANCE, RISK & COMPLIANCE SOLUTION FOR OUTBOUND EMAILS

What is SendGuard?

SendGuard is a Governance, Risk & Compliance solution for outbound emails that prevents data breaches caused by human error when sending emails.
SendGuard is used by Fortune 500 companies, multinational law and financial firms, and companies in other sectors handling confidential information to manage email risk and compliance.

HOW IT WORKS

SendGuard prompts users to confirm recipients and attachments before emails are sent. SendGuard also detects sensitive or inappropriate content within emails and applies rules based on email content and properties. SendGuard operates within Microsoft Outlook (New Outlook, Desktop, M365 OWA, and Mac) and automatically detects and prompts the user as emails are being sent.

BOOK A DEMO

CONFIRM RECIPIENTS & ATTACHMENTS BEFORE SENDING EMAILS

Get Users to confirm both attachments and recipients before emails are sent. Setup filters to control if the prompt is displayed for all emails or external emails only. External emails are color-coded for immediate identification.

DETECT, CONFIRM OR BLOCK SENSITIVE/INAPPROPRIATE CONTENT

Set DLP Rules to detect sensitive (Social Security Numbers, Credit Cards etc.) or inappropriate information (profanities etc.). Configure DLP to either get confirmation or block sending.

DEFINE YOUR OWN CHECKS/ACTIONS ON OUTGOING EMAILS

Use the SendRules engine to define your own Checks and Actions on outgoing emails. Quickly define IF/THEN conditions with an easy-to-configure interface.

UNSEND EMAILS EVEN AFTER CLICKING SEND

Automatically delay (non-urgent) emails for a minute to allow "recall" of sent emails.

KEEP LOGS FOR ADDITIONAL PROTECTION AND AUDIT TRAIL

SendGuard can also be configured to keep a log of any emails that users choose to send after a prompt is displayed.

CENTRALIZED DEPLOYMENT, CONFIGURATION AND MANAGEMENT

Configure, lockdown, deploy and manage settings using GPO, Microsoft 365 (Exchange) Admin Center or your preferred deployment tool.

CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

Vulnerability Assessment and Penetration Testing Services

Onsite | Remote

Overview of Service

Identify all 'weak points' within your organisation that are exploitable and learn how to remediate them through advanced reporting.

Remediate all 'weak points' with the assistance of penetration testers and other security experts.

HOW IT WORKS

Utilize our Pentesters as an independent service or an extension of your team - providing Penetration Tests, and Vulnerability Assessments for all of your attack surfaces.

SCOPING FORM

SCOPE

- Penetration Testing - Whitebox, Blackbox, Greybox Testing
- External Vulnerability Assessments
- Web Application Scanning
- Domain Health Scanning

BENEFITS OF VAPT SERVICES

Designed to provide businesses with essential cyber security proactive assessment services - regardless of size.

These services aims to bolster security measures, ensure compliance - with a flexible billing model.

DESIGNED FOR YOUR BUDGET

Vulnerability assessment and penetration testing (VAPT) services can be procured through two primary expenditure models: Capital Expenditure (CAPEX) or Operational Expenditure (OPEX). CAPEX involves an upfront investment in the services, or allow a Once-off fulfillment of the services. OPEX, on the other hand, entails recurring subscription fees for access to VAPT services, including ongoing support, security consultancy and remediation assistance.

REPORTING

Following a Vulnerability Assessment and Penetration Test (VAPT), comprehensive reports would be provided to the client. These reports would include detailed lists of identified vulnerabilities, their severity levels, and potential impacts on the organization. Each report would offer actionable recommendations for remediation, including specific steps to address each vulnerability. The reports would be presented in a clear and concise manner, making it easy for the client to understand and prioritize their security efforts. Additionally, each report may include an executive summary, a list of test methodologies used, and any relevant supporting documentation.

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

CYBER RISK ESSENTIALS

CYBER RISK ESSENTIALS

MANAGED CYBER AWARENESS PROGRAM

Phishing Simulations + Self-Paced Training + Instructor Led Training

Overview of Service

The Cyber Risk Essentials Suite involves Phishing Simulations, Online Training and Instructor Led Training as a multi layered service offering that enable a culture of cyber security.

HOW IT WORKS

Implement Phishing Simulations to identify non-compliant individuals within your organization and follow up with online training.

For repeat offenders, arrange Instructor-Led Training sessions with industry experts.

Ensure that your Management, Executives, and Board members receive tailored training that addresses their specific needs and concerns.

BOOK A COURSE

CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

SIMULATIONS AND TRAINING

Let CRS or CRS Partners conduct Phishing Simulations for you, or choose to manage it independently. Implement Phishing Simulation exercises with your employees to identify those who mistakenly click on harmful links.

Enhance their Cyber Awareness through Online training to strengthen their Security Mindset and help them recognize potential Cyber Attacks.

INSTRUCTOR LED TRAINING

Training for Defaulters often requires interaction with cybersecurity experts who can address their inquiries. We customize quarterly training sessions for organizations based on their geographical locations to help them comprehend the threat landscape, recognize potential threats, and respond effectively using organizational or general response guidelines for employees.

EXECUTIVE TRAINING

Executives and Board Members encounter distinct cyber challenges that often exceed the scope of typical cyber awareness training. We provide lunch-and-learn sessions on convenient days tailored for executives, allowing them to ask questions and gain insights into crucial topics. These include the effects of AI on security, deepfake technology, budgeting for cybersecurity, essential terminology, responsive measures for Executives and Board Members, and much more.

TIMELINES

- Phishing Simulations - Every 3-5 Weeks Randomized
- Online Training - Monthly and Continuous for Defaulters
- Instructor Led Cyber Awareness Sessions - Quarterly
- Executive Training - Half-Yearly

CYBER RETALIATOR SOLUTIONS

TECHNICAL TRAINING PORTFOLIO

2025

IBM COURSE BRANDS

Cyber Retaliator Solutions Delivers World-Class IBM Technical Training Globally

- Analytics
- Asset Management
- Cloud Pak for Data
- Data Security
- Digital Bus Automation
- Engineering Lifecycle Management
- IBM Security
- IBM Z - Information Management Solution
- IBM Z - Mainframe
- Identity and Access Management
- Integration & Development
- Management and Platform
- Power Systems
- Power Systems - AIX
- Power Systems - Cloud
- Power Systems - Cognitive
- Power Systems - IBM i
- Power Systems - Linux
- Spectrum Computing
- Storage
- Storage Software Technical Enablement
- Supply Chain
- Threat Management
- WFSS - Financial Crimes and Conduct Risk
- WFSS - Governance, Risk and Compliance
- Watson AI
- Instana
- Turbonomics

BOOK A COURSE

CRS
CYBER RETALIATOR SOLUTIONS

CRS will help you turn your vision into reality!
We have programs and unique delivery methods that offer choice.

www.CyberRetaliatorSolutions.com

Red Hat

Training Partner

Certified RedHat Training

Access hands-on training to stay abreast of technology trends and gain the knowledge you require to become certified. Whether you are just starting out and require Linux training or are a seasoned professional seeking automation certification, we can assist you.

BOOK A COURSE

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

SUSE TRAINING

TRAINING CATALOGUE

- SUSE LINUX
- SUSE MANAGER
- RANCHER
- HARVESTER
- NEUVECTOR
- SUSE EDGE

BOOK A COURSE

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

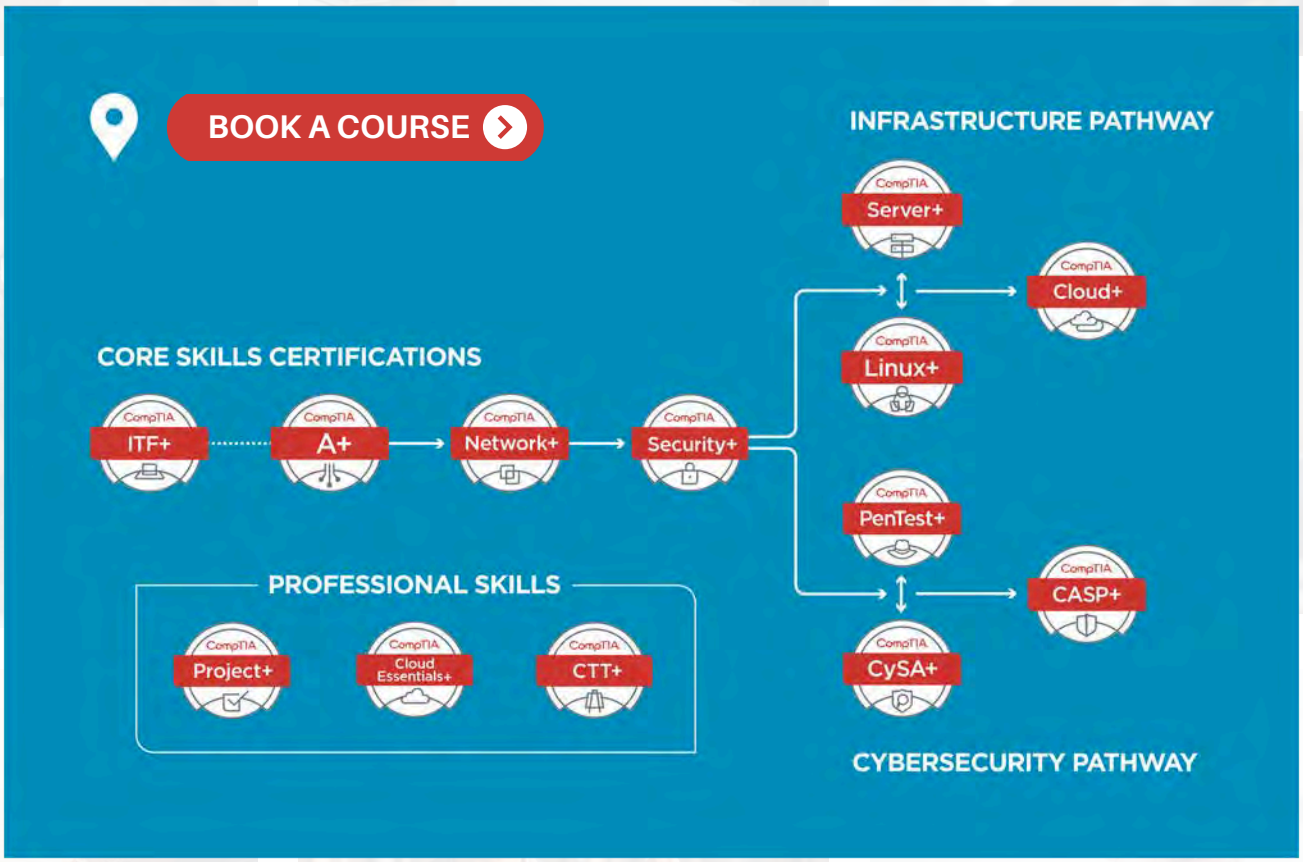
Unlock Potential

Advancing people and organizations by delivering tech talent to the global workforce.

CompTIA Authorized Partner | DELIVERY PARTNER

The CompTIA Career Pathways allow IT professionals to achieve vendor-neutral intrastructure and cybersecurity mastery, from beginning to end.

In general, the pathways follow a hierarchy of skills required for a career in IT security or infrastructure; each certification builds upon the skills acquired in the preceding one. CompTIA certifications reflect the current job roles of IT professionals, so it is logical to earn these certifications to acquire the knowledge and practical skills currently employed in the workforce, regardless of whether you have prior job experience. IT professionals and employers alike recognise that while IT certifications provide an excellent foundation, they cannot substitute for experience. By combining CompTIA certifications with on-the-job experience, you achieve the best of both worlds.



CRS CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

Agile Methodology Training

Intelligence is the ability to adapt to change

CRS
CYBER RETALIATOR SOLUTIONS

- SAFe Product Owner Product Manager
- SAFe Scrum Master
- SAFe Agile Product Management
- SAFe Advanced Scrum Master
- Leading SAFe
- SAFe For Teams
- Agile Fundamentals
- Scrum Fundamentals

BOOK A COURSE

www.CyberRetaliatorSolutions.com

CYBER RETALIATOR SOLUTIONS DELIVERS TRAINING GLOBALLY

- South Africa
- USA
- Canada
- Mexico
- Botswana
- Burundi
- Cameroon
- Eswatini
- Ethiopia
- Ghana
- Kenya
- Lesotho
- Liberia
- Malawi
- Mauritius
- Mozambique
- Namibia
- Nigeria
- Rwanda
- Seychelles
- Sierra Leone
- Swaziland
- Tanzania
- The Gambia
- Uganda
- Zambia
- Zimbabwe

CRS is an Authorized IBM Training Delivery Partner, RedHat Training Partner, SUSE Training Partner and CompTIA Training Delivery Partner.

www.CyberRetaliatorSolutions.com

CONTACT US:

Technical Training

+27 12 023 1959 - South Africa
+1 943 202 5954 - USA
Training@CyberRetaliatorSolutions.com

Distribution

+27 12 023 1959
CRSCyberSales@CyberRetaliatorSolutions.com

Head Office Address:

6D Longdale Street, Midstream Estate, Centurion, South Africa, 1692
+27 12 023 1959 - South Africa
+1 943 202 5954 - USA

Visit The CRS Website:

www.CyberRetaliatorSolutions.com