REDROK

Defending your data against the digital underworld.

RedRok deploys a strategic solution that explores the structural nature of the organization that taps into the cyclical flow of the evolving nature of risk management, technology, privacy and security.

Get insights in seconds, not hours, for quicker threat detection with one easy-to-use and comprehensive layered analysis. Providing security teams with practical guidance for threat prioritization and response.

Table of Contents

Table of Contents 2

Abstract 3

Products Suite Overview 4

1. ROKWARE – The Human Factor 4
2. INSIGHT – Eye Of The Enemy 4
3. EXSIGHT – Attack Surface Visibility 5
4. RED – Know, Not Guess 5

4.1 13

4.2 14

4.3 14

Conclusion 7

References 9

Abstract

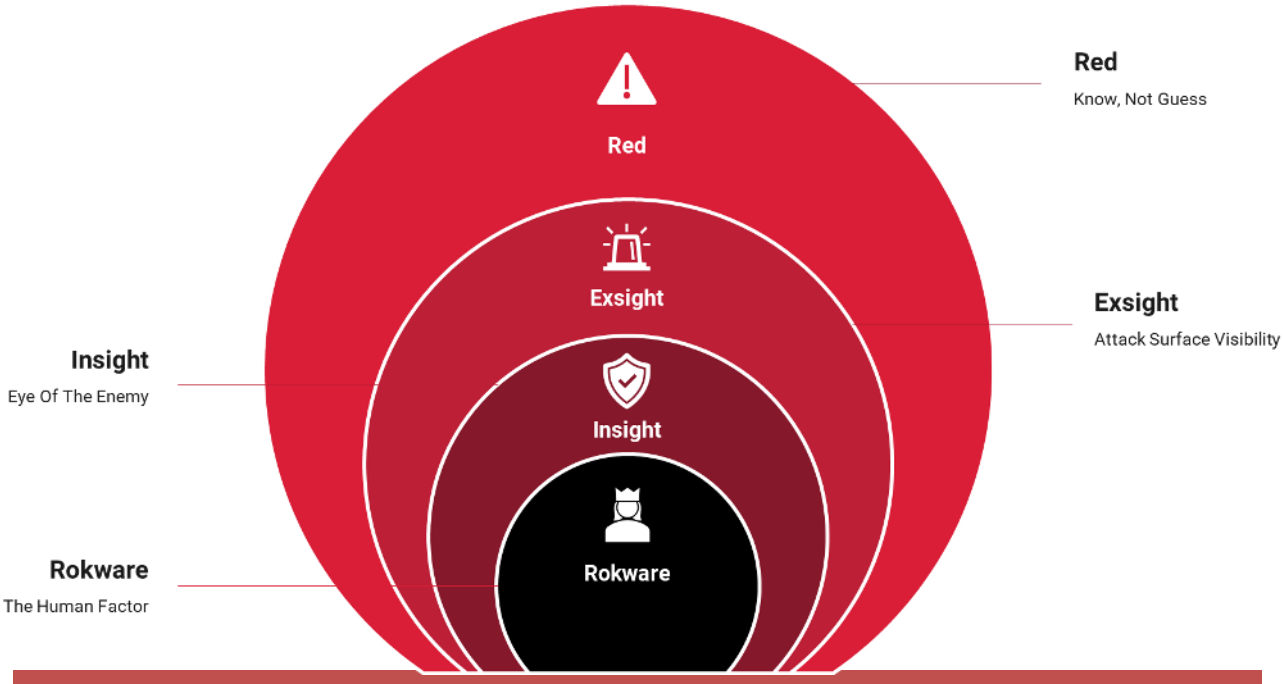
The need to secure private data and company assets has never been greater as rising threats are matched by the exponential growth of technological advancements and ever-evolving business structures. These are coupled with a dramatic increase in privacy and security regulations globally. Furthermore, the advancement in technology makes systems more interconnected offering new business opportunities. While in the past companies had separate systems for different jurisdictions, today transactions in Singapore can affect the company ecosystem in New York. A vulnerability in one place can affect the entire system globally. This has led RedRok to provide unique solutions in the world of cyber security intelligence that holistically enhances cyber protection and bolsters resilience.

We believe that there is a critical importance to organizationally aligning security systems with business operations and risk management solutions while maintaining regulatory compliance to the ever-evolving threat landscape. Our Intelligence services enables organizations to advance core strategies without compromising on strict information security requirements.

As opposed to a one-solution fits all, RedRok advances a bespoke, holistic, and deeper approach that is uniquely tailored to specific company requirements. To this end, our experts consider the organization’s strategic objectives and operational requirements to bridge the gap between vulnerabilities and resilience.

Products Suite Overview

RedRok provides unique solutions in the world of information security that holistically enhances cyber protection and bolster resilience. We offer superior end-to-end technologies that comprehensively respond to the organization's information security needs.



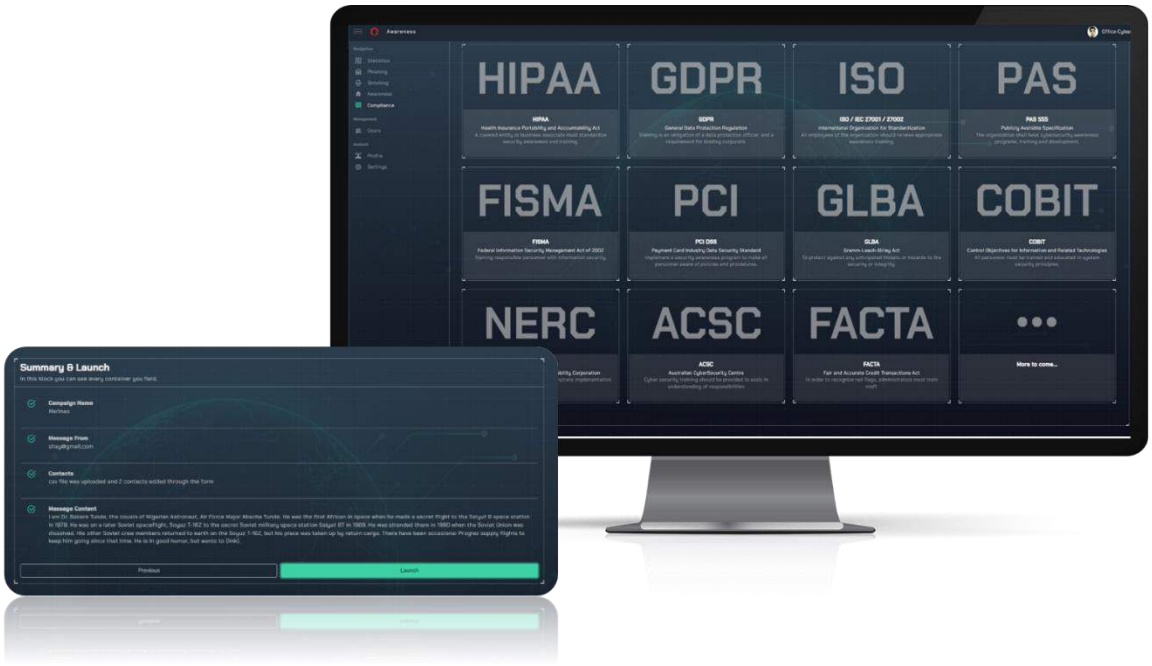
ROKWARE	INSIGHT	EXSIGHT	RED
▪ Human Factor ▪ Fully managed and automated services ▪ Cyber security awareness training ▪ Phishing / Smishing / Vishing ▪ Full GRC Support	▪ Internal Reconnaissance ▪ Obtain complete visibility ▪ Practical mitigation, compensation and offsetting ▪ AI accelerated threat detection	▪ External Reconnaissance ▪ Assets discovery and vulnerabilities (including cloud) ▪ Domains & subdomains ▪ IPs, web servers and service hunting	▪ Threat Intelligence ▪ Identify secrets & credential leaks ▪ Digital footprint intelligence ▪ Third-party intelligence ▪ Actionable threat intelligence

ROKWARE – The Human Factor

Security-conscious workforce and personnel must be more aware of safety risks to protect a legislature from hostile phishing assaults. The ability to gain a direct evaluation of staff comprehension and advancement in user behavior is made possible for organizations with RedRok technologies that provide frequent simulated phishing exercises and training.

By masquerading as a reputable business or person in an electronic conversation (usually through email spoofing, instant messaging or mobile), "phishing scams" seek to trick their targets into divulging sensitive information (such as usernames, credentials, and credit card numbers). Staff is readily vulnerable to phishing attempts, and the different strategies since attachments and email answers are regular user interactions.

Phishing exercises, which are used to increase information and educate, are an essential component of a well-developed information security management system. Identifying phishing vulnerability patterns within a department and pinpointing the need for more awareness training may be facilitated by doing continuous assessments of who is engaging in what and when in phishing emails, sms or mobile.



Rokware is a comprehensive security awareness platform that helps organizations improve their employees' knowledge and understanding of cyber security risks and best practices. The platform offers a variety of training modules that are designed to engage employees and help them learn how to identify and prevent cyber attacks. In addition, Rokware provides real-time analytics and reporting to help organizations track their employees' progress and identify areas where additional training may be needed. The platform also includes customizable content and branding options, allowing organizations to tailor the training to their specific needs and requirements. Overall, Rokware is a powerful tool for improving cyber security awareness and reducing the risk of cyber attacks for organizations of all sizes and industries.

INSIGHT – Eye of the Enemy

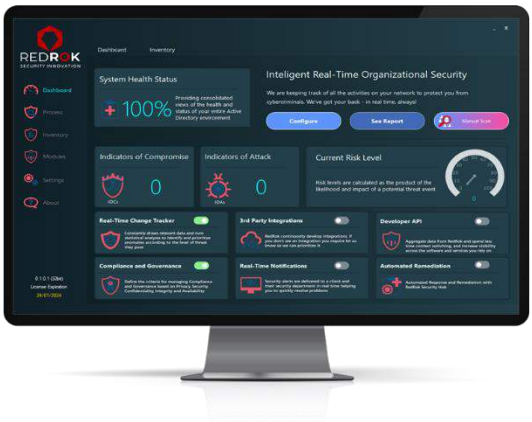
Hackers generally take a more opportunistic approach, targeting assets that are left unprotected and not considered highly valuable by the organization. Once they find an entry point, they will move through the network and continue to exploit any additional

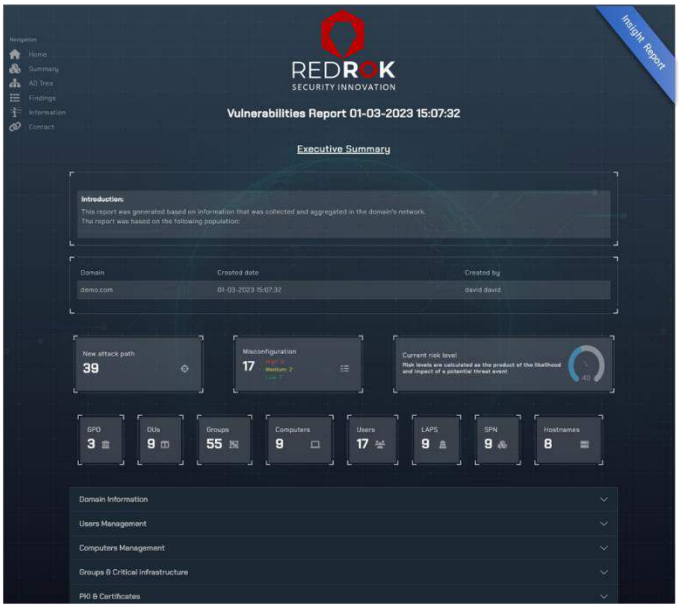
vulnerabilities they find until they can access the most valuable assets, often referred to as the "crown jewels."

Insight is an all-in-one security platform that offers consolidated and risk-based view that can be obtained in a single dashboard.

Using RedRok Insight, you can view a list of offenses that were detected in real-time, along with the MITRE ATT&CK tactics and techniques that are associated with those offenses.

With this, you can correctly prioritize the weaknesses and remediations, gain an understanding of how well you accomplish your objective to lower cyberattack risks over time and in addition, evaluate the level of maturity of the security procedures at your company to identify issue areas and enhance operational effectiveness.





1.1 INSIGHT Benefits

- **Immediate Time to Value**

Be in complete control of your IT environment and maintain each system and endpoint with an end-to-end workflow that enables you to get started on day one.

- **Understand Your Risks**

  Make sure, that all stakeholders in the company has access to an objective estimation of the organization risks they face, so that they can make better choices.

- **Build Your Security**

  Get insights in seconds, not hours, for quicker threat detection with one easy-to-use and comprehensive layered analysis.

1.2 INSIGHT Features

- **Internal Reconnaissance**
- **Obtain complete visibility**
- **Practical mitigation, compensation and offsetting**
- **AI accelerated threat detection**

- **Moving from "atomic" approach to "threat-informed defense"**

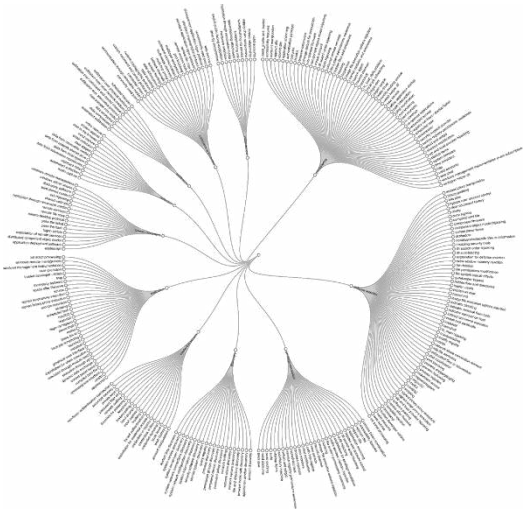
  In the past, enterprise security teams have focused on protecting their networks from specific tactics, techniques, and procedures (TTPs) used by attackers. While this "atomic" approach, which is based on analyzing real-world adversary behaviors identified in the MITRE ATT&CK® framework.
  This can be a useful starting point but it is limited in its effectiveness as a defense against threats.
  A more comprehensive approach, known as a "threat-informed defense," takes into account the full range of tactics, techniques, and procedures that an attacker may use.

- **MITRE ATT&CK and Multi-Stage Emulation**

The MITRE ATT&CK framework is a comprehensive database of tactics and techniques, based on real-world observations and threat intelligence. Many high-profile cyberattacks, such as the 2020 SolarWinds breach, are documented in the MITRE ATT&CK framework.

- **Attack Graphs in Action**

  Aligned to the MITRE ATT&CK framework, RedRok Insight emulates a range of cyber attack tactics, techniques, and procedures and enumerate complete kill-chain sequences that strings together adversary attack graphs



2. EXSIGHT – Attack Surface Visibility

Exsight is an innovative security platform that provides comprehensive external reconnaissance capabilities to help organizations identify and mitigate security risks. This fully SaaS platform is designed to be easy to use, with a user-friendly interface that makes it simple to access and analyze critical security data.

One of the main features of Exsight is its asset discovery and vulnerability scanning capabilities. With this feature, organizations can quickly identify all of their assets, including those in the cloud, and assess their security posture. The platform's vulnerability scanning capabilities provide detailed information about potential exposed

vulnerabilities, allowing organizations to prioritize remediation efforts and improve their overall security posture.

In addition to asset discovery and vulnerability scanning, Exsight also includes powerful domain and subdomain discovery capabilities. This feature allows organizations to quickly identify all of their domains, subdomains, IP, API and more, including those that may be hidden or obscure. By identifying these domains and subdomains, organizations can better understand their attack surface and take steps to mitigate potential security risks.

Exsight is an essential tool for any organization that takes security seriously. organizations can better protect their assets and ensure the security of their data and networks.

2.1 EXSIGHT Benefits

- **Comprehensive Security Solution**

  Exsight offers a complete security platform that includes asset discovery, vulnerability scanning, domain and subdomain discovery, and more. This all-in-one solution helps organizations streamline their security processes and identify risks more effectively.

- **Easy-to-Use Interface**

  The user-friendly interface makes it simple for users to navigate and analyze critical security data, ensuring that organizations can get the most out of the platform without any technical expertise required.

- **Enhanced Visibility:**

  Exsight's asset discovery and domain/subdomain discovery capabilities provide organizations with a clear picture of their entire digital footprint, including cloud assets, IPs, APIs, and other critical components. This improved visibility enables organizations to better understand their attack surface and implement effective security measures.

- **Prioritized Remediation**

  By identifying exposed vulnerabilities and providing detailed information about them, Exsight helps organizations prioritize their remediation efforts, ensuring that the most critical risks are addressed first.

- **Continuous Monitoring**

  Exsight's SaaS platform allows for continuous monitoring and updates, ensuring that organizations always have the most up-to-date security information and can quickly respond to emerging threats.

- **Scalability**

  Exsight is designed to grow with your organization, easily scaling to accommodate expanding infrastructure and increasing security needs.

- **Cost-Effective**

  As a fully SaaS platform, Exsight eliminates the need for expensive hardware, software installations, and maintenance, reducing the overall cost of securing your organization.

- **Improved Compliance**

  Exsight's comprehensive security capabilities can help organizations meet and maintain compliance with various industry regulations and standards, reducing the risk of fines and penalties.

- **Enhanced Security Posture**

  By providing organizations with the tools to identify and mitigate security risks, Exsight helps improve their overall security posture, protecting their assets, data, and networks from potential threats.

- **Proactive Threat Management**

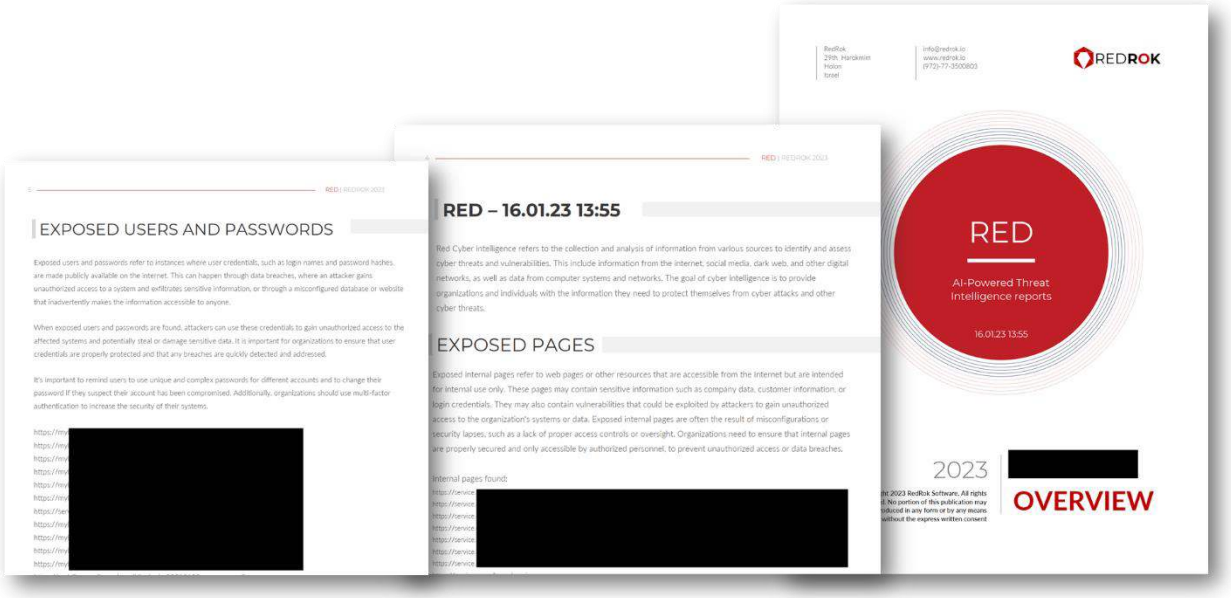
  With Exsight, organizations can be proactive in their security efforts, identifying and addressing risks before they can be exploited by malicious actors. This proactive approach can save time, money, and potentially prevent devastating security breaches.

3. RED – Know, Not Guess

Red Cyber Intelligence Services aim to help individuals and organizations to protect themselves from cyber threats by gathering, analyzing, and transforming data into actionable intelligence. The service considers at least three approaches for controlling and protecting digital exposure. By utilizing identification data, the intelligence gathered can enable proactive measures to enhance digital security.

In cyber intelligence, it is important to identify trends specific to an organization to narrow down the threats that are relevant to them. By analyzing trends and patterns of cyber threats and attacks that are specific to an organization, cybersecurity

professionals can focus their efforts on protecting against those threats that are most likely to impact the organization.



3.1 RED Benefits

- **Improved incident response**

  Red helps security teams respond to security incidents more effectively by providing real-time alerts, automated workflows, and recommendations for remediation actions.

- **Proactive threat hunting**

  Red assist in proactively identifying potential threats before they cause significant harm. This can help organizations stay ahead of the attackers and prevent security incidents before they happen.

- **Build Your Security**

  Faster and more accurate threat detection. Red analyzes vast amounts of data from various sources to identify security threats.

3.2 RED Features

- **Red Threat Data Feed Service**

  A subscription-based service that provides an organization with up-to-date information on potential cybersecurity threats to identify and alert the organization of potential threats.

- **Digital Footprint Intelligence Services**

  This service provides insights into an organization's online presence, vulnerabilities, and threats. It enables proactive cybersecurity measures to mitigate risks and protect assets.

- **Red Dark Web Hunting Service**

  Red monitors, searches and identifies the dark web for any stolen, leaked, or compromised data belonging to an organization that may pose a threat to the organization.

- **Advanced Persistent Threat Intelligence**

  Collection, analysis, and dissemination of information related to advanced persistent threats (APTs) that target an organization. Detailed insights into the techniques, tactics, and procedures of APT groups.

3.3 Threat Intelligence Sources

- **ISACs, commercial and government intelligence sources**
  - **Commercial threat intelligence providers:** These are companies that specialize in collecting and analyzing threat intelligence data and providing it to organizations for a fee.
  - **Government agencies:** Many governments provide cyber threat intelligence services to their citizens, either through official channels or via public-private partnerships.
  - **Information sharing and analysis centers (ISACs):** These are industry-specific organizations that share threat intelligence data and best practices among their members.

- **Red security research team, open-source and communities intelligence sources**
    - **Open-source intelligence:** Publicly available information that is used to gain insight into potential cyber threats. This includes sources such as social media, news reports, and blogs.
    - **Online threat intelligence communities:** Online communities where cybersecurity professionals and researchers share threat intelligence data and discuss the latest threats.
    - **The Red Security research team:** A group of experienced professionals who specialize in analyzing threat intelligence data and identifying the latest cyber threats to help organizations stay secure.

Conclusion

We introduced RedRok cyber security tools that can help organizations identify and mitigate potential security risks.

Rokware is an awareness platform that provides cyber security training, phishing/smishing/vishing prevention, and full GRC support.

Insight is an internal reconnaissance tool that offers complete visibility, practical mitigation, compensation and offsetting, and AI-accelerated threat detection.

Exsight is an external reconnaissance tool that can discover assets and vulnerabilities, identify domains and subdomains and IPs, and hunt web servers and services.

Finally, Red is a threat intelligence tool that can identify secrets and credential leaks, provide digital footprint intelligence, third-party intelligence, and actionable threat intelligence.

These tools can be used together to create a comprehensive cyber security strategy and protect organizations from various security threats. e conclusion is an opportunity to briefly recap what you covered without sounding repetitive.