INFOVISION
#AccelerateDigital

Whitepaper

Red teaming for cybersecurity

2024 is the year to invest

—

This whitepaper offers a comprehensive exploration of Red teaming for cybersecurity professionals and decision-makers, focusing on its significance in 2024. It explores the benefits, challenges, best practices, and trends in Red teaming, along with real-world insights across industries.

The cyberthreat landscape has evolved. Are you evolving with it?

In August 2022, password management service LastPass suffered a high-profile cyber attack. The attacker accessed a LastPass software engineer's corporate laptop and stole highly sensitive data, including some of the company's source code. In November of the same year, the company suffered another significant attack in which encrypted and unencrypted user data was compromised. The fact that companies in the business of keeping users safe online can be vulnerable to breaches underlines how vital cybersecurity is today.

Outside of reputation damage, the impact of data breaches on balance sheets is significant. IBM estimates that the average cost of a data breach is $4.45 million, which has increased 15% in a three-year period.

Increased reliance on digital solutions comes with a corresponding increase in the potential for financial and reputational risk from cyber-attacks. This makes cybersecurity investments necessary for businesses of all sizes with significant digital exposure. This trend is reflected in the growth of the cybersecurity market, which is expected to reach $350.23 billion by 2029, growing at a CAGR of 11.44% during the forecast period (2024-2029).

The case for Red teaming

As cyber threats become more advanced and potential for disruption increases, more businesses are turning to high-level cybersecurity practices. One such approach is Red teaming. Additionally, Red teaming is becoming increasingly relevant in today's cybersecurity context due to its ability in meeting regulations like GDPR, PCI DSS, and NIST standards.

Red teaming 101

What
is Red teaming?

- Red teaming is a form of ethical hacking that simulates real-world cyberattacks on an organization's own systems, processes, and people.
- The exercise is designed to identify blind spots in defense systems by thinking like the people looking to bypass them.

How
does it work?

Red teaming can be performed using various methods and techniques, such as:

- **Penetration testing:** A systematic attempt to exploit vulnerabilities in an organization's network, systems, or applications.
- **Social engineering:** A manipulation of human behavior to gain access to information or resources.
- **Physical security testing:** A breach of an organization's physical premises or assets.
- **Business process testing:** A disruption or compromise of an organization's critical business functions or operations.
- **Cyber threat intelligence:** A collection and analysis of information about current or potential cyber threats or adversaries

Why
choose Red teaming?

- The goal of Red teaming is to test the effectiveness of an organization's security posture, identify vulnerabilities, and provide solutions.
- It can also help organizations prepare for the worst-case scenarios, such as ransomware attacks, data breaches, or cyber espionage.

* *General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST).*

Why does simulating advanced adversaries matter?

As Red teaming is only as effective as the methods used to penetrate an organization's defenses, simulating modern tactics leveraged by an experienced adversary is critical.

However, not all Red teaming exercises are created equal.

Advanced adversary simulation, a proven approach, emulates the tactics, techniques, and procedures (TTPs) of real-world adversaries that pose a high risk to an organization.

Methodology

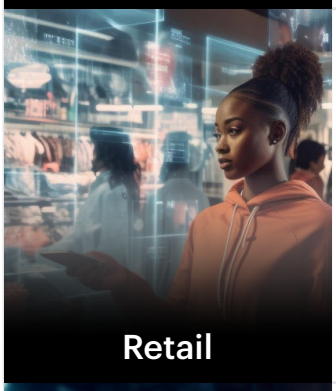
Threat modelling: Threat modelling is the process of identifying and prioritizing the potential threats that could target the organization, based on its assets, vulnerabilities, and adversaries. Threat modelling helps to understand the attacker's motivations and methods and define realistic attack scenarios that align with the organization's business objectives and risk profile.

Existing intelligence on adversaries: Red teams use existing intelligence about actual adversaries to inform simulations. This includes emulating the tactics, techniques, and procedures (TTPs) of known threat actors. Red teams can leverage open-source intelligence (OSINT), commercial threat intelligence feeds, and internal security data to identify relevant indicators of compromise (IOCs).

Balancing hypothetical vs. intelligence-driven scenarios: While it is important to simulate known adversaries and their methods, it is also essential to account for unknown or emerging threats that may not be predictable based on existing intelligence. Red teams use creative and innovative techniques to simulate advanced adversaries that could bypass or evade existing security controls.

How Red teaming elevates safety across mission-critical industries?

Here's a concise overview of our Red teaming interventions across the industry spectrum

Industry	Why Red Teaming matters?	Red Teaming approach	Red Teaming outcomes
 BSFI	Persistent cyber threats due to valuable data. Compliance with regulations like the GDPR and PCI DSS to avoid fines and reputational damage.	Test online banking and network security through simulated attacks. Asess transaction processing systems' and customer data protection's resilience.	Enhanced security with multi-factor authentication and encryption. Quicker breach detection and response, minimising impact and cost.
 Healthcare & Life Sciences	Cyber attack risk from digital health records and devices. Patient data protection is vital, with regulations like HIPAA in the U.S. and GDPR in the EU.	Simulated attacks on electronic health record systems to assess security and privacy. Test the security of IoT medical devices and hospital networks to identify potential vulnerabilities.	Enhanced defense against data breaches with encryption, access control, and backup. Increased security protocols with patching, monitoring, and segmentation.
 Retail	Large customer and payment data at risk of hacking. e-commerce growth increases transactions and attack vectors.	Imitate cybercriminals targeting online payment systems for fraud/theft. Social engineering to trick employees into disclosing sensitive data or credentials	Enhanced security for e-commerce and payment systems. Boosted employee vigilance and defense against phishing and social engineering.
 Manufacturing	Be vigilant about automated and connected systems. Manufacturers need to protect their intellectual property and trade secrets from competitors	Mimic hackers attacking ICS and supply chain networks. Aim to leak intellectual property and trade secrets.	Enhanced security measures for industrial control systems. Increased protection of intellectual property and sensitive company data

* *BFSI (Banking, Financial services and Insurance), General Data Protection Regulation (GDPR) Payment Card Industry Data Security Standard (PCI DSS), The Health Insurance Portability and Accountability Act (HIPAA), industrial control systems (ICS)*

AI & ML in Red teaming

While Red teaming is highly effective in identifying gaps and blind spots in the security infrastructure, it is a complicated and time-consuming exercise. Practical Red teaming exercises require a lot of expertise, resources, and time to design, execute, and analyze complex cyber threat scenarios. Red teaming can also be challenging to scale and automate when dealing with large and dynamic systems.

This is where artificial intelligence (AI) and machine learning (ML) become crucial. AI and ML are not only making cyber-attacks more advanced, but they can also be the perfect antidote for automating defensive efforts against them.

When Google attempted to steal Google Glass from itself

In an intriguing exercise, Google's internal Red team launched a unique challenge to test the security of Google Glass around its 2013-14 launch. They crafted a benign-looking email discussing ergonomic postures for office workers, exploiting a mix of social engineering and the potential of AI tools, to mimic threats that could bypass security measures, including biometric systems. Their efforts culminated in a successful breach through a malware-laden USB, leading to the swift patching of this vulnerability. This operation highlights the critical pace at which red teams operate and the continuous evolution of cybersecurity defenses, inspiring Google to share their solutions to bolster protection against similar threats industry-wide.

AI in Red teaming

- Natural language processing (NLP) generates realistic content for phishing emails, fake websites, or social media posts.
- AI-driven automation assists with routine tasks such as data analysis, vulnerability identification, exploit development, and payload delivery.

ML in Red teaming

- Machine Learning models trained on network logs, security alerts, and threat intelligence feeds can help generate advanced threat scenarios
- Data mining and pattern recognition allow Red teams to sort through large datasets and iterate quickly

It is important to underline that AI and ML are not silver bullets for Red teaming. They still require human oversight, guidance, and validation to ensure accuracy, reliability, and ethics. Red teams must have an in-depth understanding of the models they use to avoid introducing new vulnerabilities, accidentally.

Red teaming trends & predictions

Red teaming trends & predictions

As more advanced technologies emerge into 2024, Red teaming will face challenges and opportunities that require evolved approaches. We bring out some key trends along with predictions for the future of Red teaming.

Trend 1: Increasing integration of AI and ML

AI and ML can help automate the generation and execution of attack scenarios and adapt to the changing environment and defenses of the target organization. According to Microsoft, even machine learning systems can be compromised by adversarial samples, data poisoning, model theft, and other techniques that exploit their limitations and biases. To counter this, Red teaming will need to incorporate sophisticated methods.

Trend 2: Red teaming as a regular security practice

With the potential for business disruption and financial downside increasing, organizations will conduct red team tests more frequently and continuously. Red teams will need to use agile methodologies to plan, execute, and report on their tests in short cycles. With automation, historical data, and feedback from blue teams, red teams in 2024 can craft sophisticated scenarios to push the boundaries of cybersecurity.

Trend 3: Specialized red team partners

Organizations will collaborate with specialized Red teams offering niche skills in specific domains, such as cloud, IoT, or mobile security. These partners will help organizations simulate more realistic attacks and provide in-depth vulnerability assessments. Bodies like the European Banking Authority (EBA) strongly recommend security measures like red teaming to financial institutions to assess their resilience against advanced persistent threats (APTs).

Trend 4: Red teaming beyond networks and applications

As IoT devices like smart speakers, cameras, thermostats, locks, and wearables gain popularity, the surface area for attackers to exploit also increases. IoT devices often have weak security configurations, outdated firmware, default credentials, or unencrypted communications that can expose the networks they connect to or compromise the device's functionality. In 2024, red teams will look to find critical vulnerabilities introduced by such devices.

Trend 5: Red teaming in non-traditional industries

A lot of new industries are adopting digitization thus getting exposed to cyberattacks. Industries such as agriculture or transportation will start recognizing the need for Red teaming. These industries often rely on legacy systems or proprietary protocols not designed with security in mind. Given the severe consequences for human safety or environmental impact posed by cyber-physical attacks on these industries, it is essential for them to consult with cybersecurity experts proactively.

Trend 6: Red teaming will be a part of overall security posture

In 2024, security experts will elevate the importance of Red teaming as an integral part of an organization's security protocols. Given the increasing number of attack vectors available, in-house security teams will work with experienced red team partners to cover potential gaps in their skill sets and develop comprehensive security coverage.

Trend 7: Expansion of regulatory compliance and standards

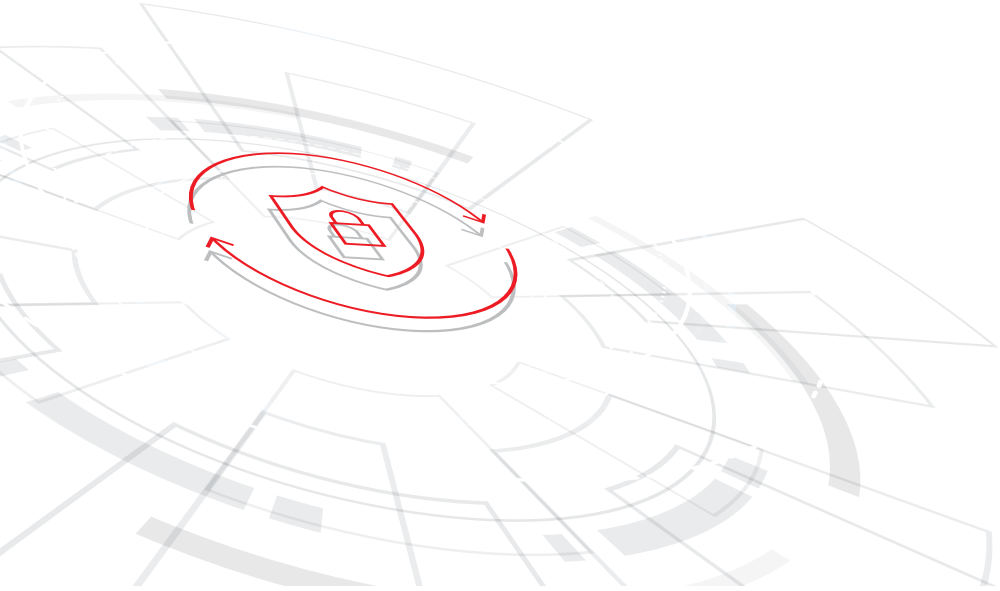
Organizations will collaborate with specialized Red teams offering niche skills in specific domains, such as cloud, IoT, or mobile security. These partners will help organizations simulate more realistic attacks and provide in-depth vulnerability assessments. Bodies like the European Banking Authority (EBA) strongly recommend security measures like Red teaming to financial institutions to assess their resilience against advanced persistent threats (APTs).

Trend 8: Emergence of red teaming as a service (RTaaS)

Red Teaming as a Service (RTaaS) will emerge as a critical offering for businesses lacking in-house capabilities. RTaaS is a new model that combines the best aspects of human-led Red teaming with modern technologies that incorporate AI, automation, and cloud-based SaaS controls.

Trend 9: Enhanced employee training and awareness programs

Simulated attacks will serve as practical learning experiences for staff, improving security awareness. Red teaming will also help foster an organizational security culture where employees are encouraged to report suspicious activities and incidents.



Best practices

Do’s and don’ts of Red teaming

Do’s

Conduct regular red team assessments to simulate and uncover vulnerabilities and weaknesses in your security defenses.

Set clear objectives for red team exercises to ensure well-defined goals and expectations.

Use realistic threat scenarios that mirror actual cyber threats your organization might face.

Document everything meticulously, including findings, actions, and lessons learned, to improve future security efforts.

Respect legal and ethical boundaries by obtaining proper permissions, respecting privacy, and staying within legal frameworks.

Don’ts

Don't ignore physical security, as it is critical to overall security posture.

Don't overlook non-technical staff; they can be vectors for social engineering attacks.

Don't use outdated techniques, as they may not accurately reflect modern attack vectors.

Don't disrupt business operations during red team assessments; prioritize minimal impact.

Don't "set it and forget it" by neglecting follow-up and continuous improvement after assessments.

Kickstart your red team implementation with InfoVision

By implementing Red teaming in 2024, you can gain a 360-degree view of your security posture, test your defenses against the latest attack techniques, train your security team, and prioritize your security investments.

According to IBM, only 28% of organizations leverage security AI and automation extensively, despite the potential to enjoy average savings of nearly $2 million.

How InfoVision can help

InfoVision is a leading digital technology services company with nearly three decades of experience helping businesses with digital transformation and security. Our approach to cybersecurity prioritizes proactive methods like Red teaming over reactive measures like vulnerability scanning. This focus on advanced threat simulation has made Red teaming a sought-after offering among InfoVision's Industrial Automation, Intelligence, and Digitalization services.

Access industry-leading cybersecurity expertise

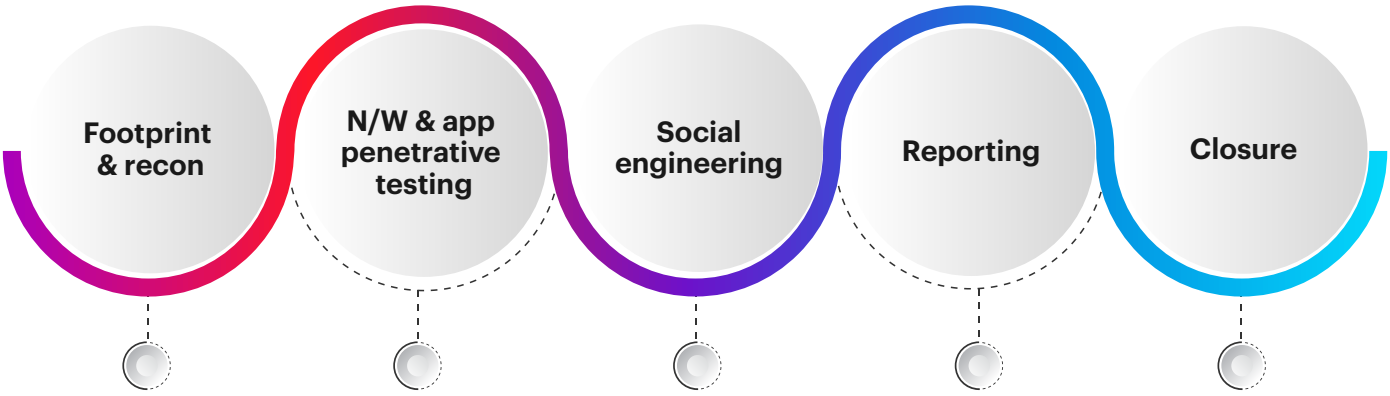
Infovision's cybersecurity professionals hold CEH, CPENT, SANS, and OSCP credentials. Our red team's cross domain expertise allows for sophisticated exercises that are comprehensive and resource-efficient compared to regular penetration testing.

Proven Red teaming track record

Infovision has undertaken 21 successful Red teaming projects across diverse industries — including finance, healthcare, and manufacturing. Regardless of your industry, Infovision's combination of specific and agnostic techniques can mimic modern cyber-attacks.

How Red teaming elevates safety across mission-critical industries?

Here's a concise overview of our Red Teaming interventions across the industry spectrum:



Passive & active recon

- OSNIT
- Priotitize attack oppurtunities

Exploit & establish

- Initial access
- Identify & exploit vulnerabilities
- Lateral movement

Adversary emulation

- Credential Management
- Security Awareness
- Multiple security levels
- Prevent exfiltration
- Expose weak processes

Documentation

- Executive summary
- Recommendations
- Detailed assessment report

Takeways

- Closure of vulnerabilities by client
- Confirmation testing

In 2024 and beyond, let Infovision empower your organization with proactive Red teaming strategies. Conduct effective and efficient Red teaming exercises without the need for complicated resource deployment and improve your overall security posture. Together, we can protect your organization's assets and pave the way for a secure and resilient future.

Sai Surapaneni
Global Practice Head
Enterprise Cybersecurity & Risk Services

Author

Sai is a cybersecurity expert and is passionate about building world-class security services. At InfoVision, Sai is responsible for capability building and heading the Enterprise Cybersecurity & Risk Services' Center of Excellence. With over 15 yrs of experience, Sai has multiple organization-wide certifications including PCI DSS, HIPAA, SOX, ISO 22301, ISO 27001 and ISO 9001.

#ACCELERATEDIGITAL

Reach out on for a non-obligatory discovery discussion.