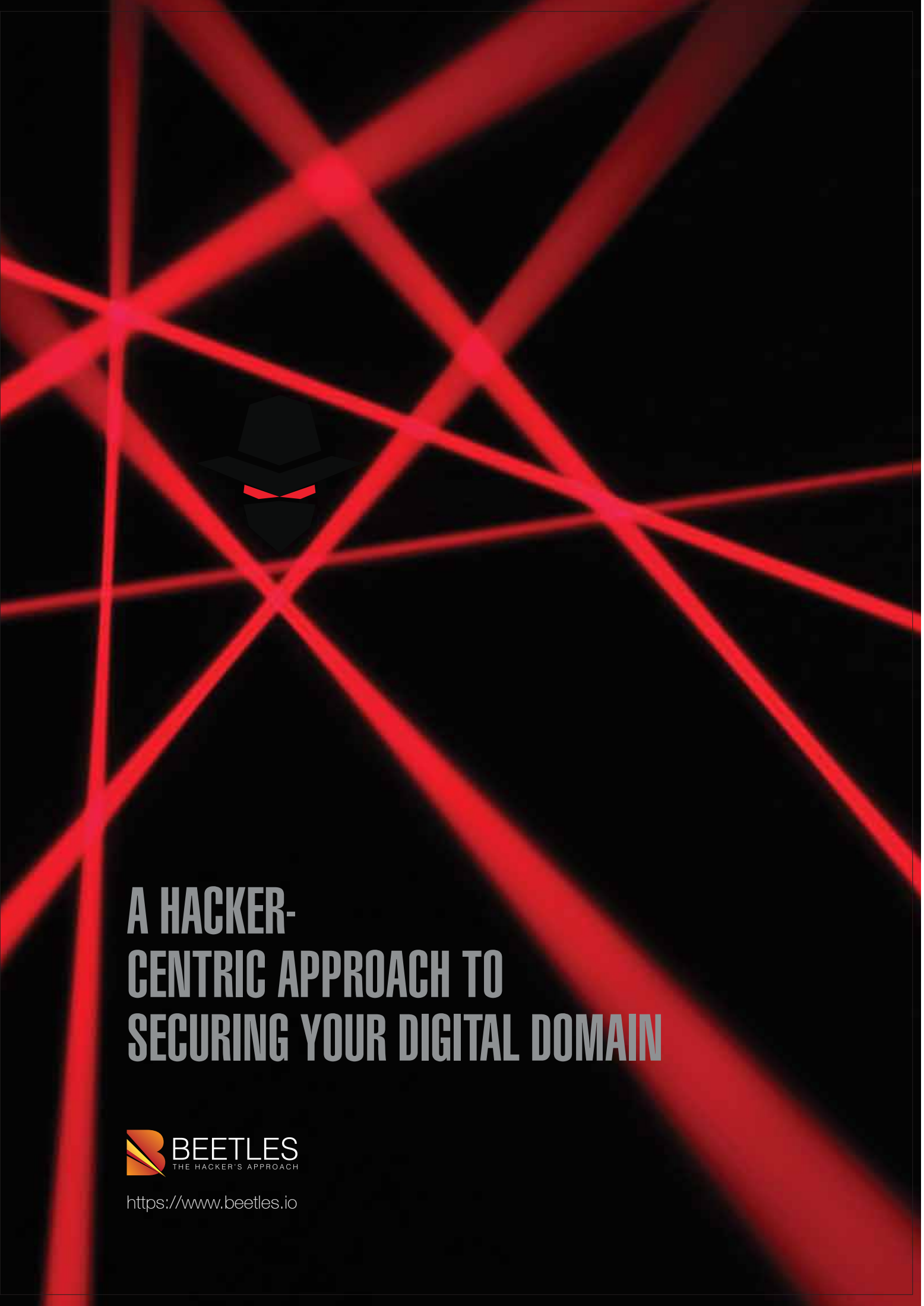


A HACKER-CENTRIC APPROACH TO SECURING YOUR DIGITAL DOMAIN

BEETLES
THE HACKER'S APPROACH

https://www.beetles.io


SAFETY
Password
Protection
likes
Security
Code
dislik
financial
history
friends
PERSONAL DATA
Data
INFORMATION
Information
Data
Privac
PRIVACY
Security
SAFETY
Protection
Password
FRIENDS AND FAMILIES
financial history
SECURITY
Data
Code
Protection
information
likes and dislikes
PROTECTION
SAFETY
families
Information
Protection
Informatio

Beetles

The Internet is infinite, but still growing every day. It has given rise to new opportunities in every field imaginable, be it business, entertainment, education or otherwise. Our entire lives have been neatly packaged and upload in a digital version of ourselves. All our personal data, our friends and families, our likes and dislikes, even our financial history and current data are stored in invisible packets in the vast openness of the world-wide web. For our own ease of access, we have digitalized our entire businesses, where we prefer to store even the most sensitive information in these packets, all our trade secrets, our financial data, our vulnerabilities and our opportunities.

The internet has been a boon and an inseparable partner in our modern lives, but it has its own disadvantages as well. Criminals are now faceless and seemingly traceless. **The bigger weapon now is not a gun, but a keyboard**. From malicious codes to Trojans to phishing and organized crimes (data theft, DoS, DDoS) are the new threats we face every day. The new criminal hides in the Deep Web, without a face or a name, waiting, only but a keystroke away.

To face these threats and minimize damage, we bring a multi-platform security solution with our highly versatile and globally accredited team. So, relax and let us secure the system and services that power your business.

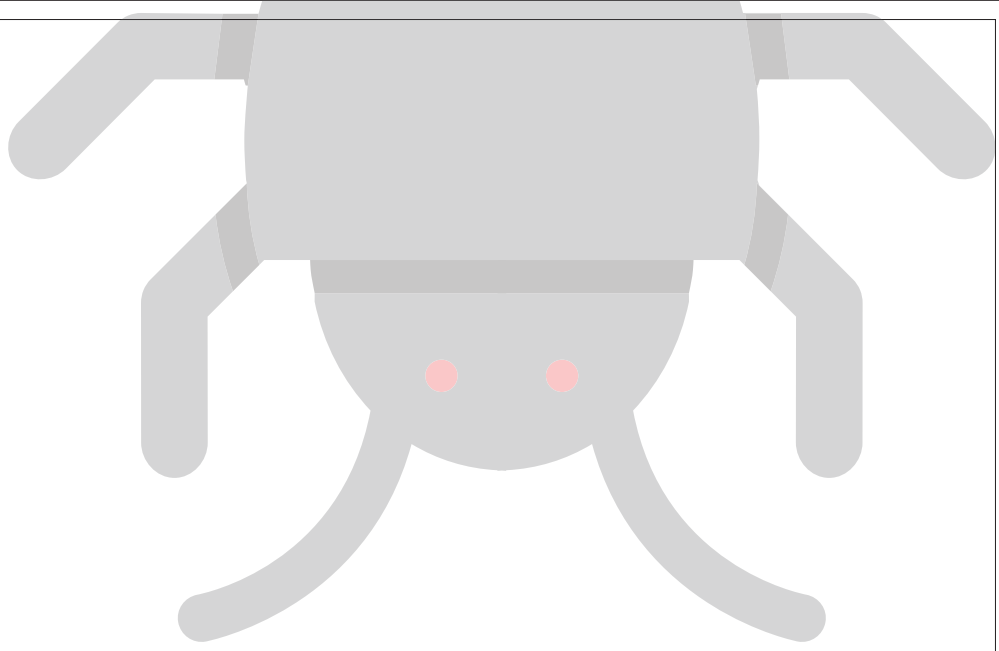
As threats are increasing, the danger of coming under attack is imminent. Beetles has been created with the sole purpose of warding off these criminals, safeguarding the clients' data, both personal and professional from such attacks, ensuring that no Revenue Impact or Business Impact befall the client. Carefully selected and rigorously vetted researchers from our global resource pool make up the Beetles Red Team and they have been structured and molded in such a fashion, always vigilant, always protecting. They are strong, versatile and sharp, like the tip of a dagger!

BEETLES

We provide you with a hacker's point of view in hardening your systems

Our services are
variable and customizable,
as are the **costs**!

You can rest assured knowing
your security is in good hands.



Why is it so important to enforce cyber security?

In our modern era of digital communication and trading more and more unique opportunities are appearing for starting and growing businesses, government institutions, academic institutions and various others. However, these seemingly significant advantages overshadow the fact that, these potential benefits come hand in hand with potential threats as well. Sadly, in haste, people ignore or overlook these deadly threats which could lead them to incur heavy financial or business losses. As The Telegraph, a UK based newspaper reported, "**Cyber crime** costs global economy **$445 Billon** annually" *and Forbes, the renowned business magazine, projected the growth of the cyber security industry to USD 170 Billion, annually, by 2020*.

Ransomware

Among the most threatening cyber-security threats of the recent years, Ransomware is probably the most known and feared. Hackers, or the threat actor, can infect any system with this malware by exploiting existing vulnerabilities in the system. True to its name, ransomware holds the essential data of its victims as hostage until a ransom is paid. A report by Aljazeera stated that over 200,000 devices were affected during the recent ransomware attack in June 2017 and **this will become more of a threat in the future.**

Identity Theft

Impersonating another individual's identity to steal money or committing other crimes has been a major issue much before the inception of the Internet and the digitalization of our identities and banking system has made it very accessible for cyber criminals to steal your identity by various means. **These criminals, by hacking into your laptops or mobile phones**, will gain access to your credit card or banking account information potentially use that information to mishandle your money. Phishing attacks, accessing unsafe networks and many other factors lead to identity theft.

Distributed Denial of Service (DDoS)

One of the most widespread types of cyber-threats, DDoS, represents a great dilemma for governments and institutions today. These intrusions are focused on online service providers (e.g. ISP, news provider) as their businesses depend on the availability of their web sites for critical business functions and productivity. Due to lack of experts in building defense for DDoS many corporations are falling victim to this threat.

(Trivia Info: Kaspersky revealed, that although the first quarter of 2017 was rather quiet compared to the previous reporting period, there were a few interesting developments. Despite the growing popularity of IoT botnets, Windows-based bots accounted for 59.81% of all attacks)

Cyber Security Consulting

Learn about different threats and how best to mitigate them

Know thyself, learn about the threats which are more likely to befall your business specifically. After carefully analyzing the key areas of your business, people, process and technology, our team of security experts will advice you about which approach is the safest and which approach is the most cost-effective. Consequently, you will have no need to worry about spending too much on the security or too little with the help of our cyber security consultancy experts.

People

1 Firewalls, patches and passwords are only a part of cyber security. Most of the problem lies with the human factor. People misplace their passwords, access potentially harmful domains and are negligent about their important data. We will give them proper security knowledge, help construct strong policies and increase awareness so that chances of breach are reduced.

Process

2 The next step is consulting about the processes of your business which are electronically integrated so that they are not ineffective or vulnerable to outside threats.

Technology

3 Technology is what we do best. The team will refer your business to your proprietary Beetles Platform, where we can initiate a deep-dive into your systems and applications, in what we call The Hacker's Approach.

Source Code Auditing

Analyze, debug and patch the source code for important programs

Many companies face severe issues when essential software and programs for business functions (e.g. search engines, Customer relationship interface) break down, have bugs and restart constantly. However, not to worry, with the help of our remarkable team a Source Code Security Audit can be conducted where experts manually inspect the source code of your new or existing application on a line-by-line basis, for security weaknesses, review authentication, authorization, session and communication mechanisms. They will identify issues that could result in unauthorized access or leaking of sensitive information.

The audit can be done immediately post-deployment but it is recommended that you incorporate us in your SDLC for a better and secured development process.

Vulnerability Assessment

Assess your defense against hackers

It is very common for electronic devices and endpoints, networks or any communication infrastructure to be vulnerable to outside attacks. Vulnerability assessment is defining, identifying and classifying any security holes or breaches in these devices and infrastructures as well as forecasting the effectiveness of proposed counter-measures and evaluate their actual effectiveness after they are put into use.

This is a non-exploitive (does not breach your systems) test. Performed on individual IP addresses or nodes owned by your company, this test will be only done on the IP addresses that you designated.

(Trivia Info: One of the most used web application for constructing web pages, WordPress, has plug-ins which has some of the biggest vulnerabilities in the internet.)

Internal & External Penetration Testing

Look through the eyes of a hacker

Ever wonder how hackers steal **Information**, access your **Security systems** and decrypt **Databases**? Through a Penetration Testing engagement, we will show you exactly how the hackers gain access and which information they have access to. This is separated into two categories.

With External Penetration Test, which is the first layer of your system, our team will mimic hackers and the process they would go through to exploit the weaknesses in your application's security, in what we call, "The Hacker's Approach". Additionally, weaknesses in the external IT systems are identified which could be used to disrupt confidentiality, availability or integrity of the network, thereby allowing you to rectify them. Some of the methods used in these tests are:

- Sensitive Information Disclosure
- Crafted Penetration Testing
- Probing Different Services
- Intrusion Detection and Prevention System Testing
- Password Service Strength Testing

In contrast, Internal Penetration Test, the second and third layer, demonstrate how a rogue insider in your organization (if any) will exploit the vulnerabilities of your internal security system. Even though it might sound unlikely, most of the cyber-crime conducted across the world happen because of internal security flaws. Our methods for running this test are:

- Scanning the Internal Network
- Password Service Strength Testing
- Firewall Configuration Review
- Application Security Testing
- Elevation of Privilege
- Network and Security Control Testing

Holistic Audit

Know about weaknesses outside computers and electronic devices

Security of your information isn't restricted to your devices and networks, your programs and the expertise of your programmers. It is a very wide prospect which encompasses your employees, the nature of your organization, security training and many other factors. So, we propose a holistic audit which goes beyond the immediate cyber domain to deliver a complete 360-degree security assessment of your organization, including human and environmental factors. Consequently, you will be provided with an extensive report portraying all the vulnerabilities across your organization as a complete entity. In addition, we will provide you with different recommendations so that you can choose the one which suits your organization the most. By the end you will be able to correctly comprehend the status of your information security and make informed business decisions about it.

(Trivia Info: The biggest breach of security in US history happened in 2013 when highly-classified information was released to the public by Edward Snowden. Surprisingly, he didn't hack or input malware or do anything complicated, he just uploaded data to a thumb-drive and carried it out. The rest is history.)

Digital Forensics

Reconstruct a digital crime to find out what information hackers stole or damaged

Often hackers breach into a system and get out without seemingly doing any sort of harm. However, they may leave dangerous malware which may be triggered in the future, resulting in terrible consequences. Moreover, there may be occasions where you have been breachel but can't identify what data was stolen, destroyed or manipulated. On such occasions, our team will conduct a digital forensic analysis to see exactly how the hackers breached into your system and what their goal was. Through a careful step-by-step approach, we will reconstruct the crime and present digital evidence. In a time where digital information is integrated to every part of business processes, legal and administrative issues, knowledge about breach in your system might be the critical factor which saves your organization from potential downfall. Some functions of digital forensics are:

1 Indicators of Compromise (IoC)

These are pieces of forensic data found in log entries or system files, made primarily of virus signatures, IP addresses, URL domains, hash values. They are created by experienced analyst through multi-step processes based on past statistics and knowledge.

2 Indicators of Attack (IoA)

These are series of activities done by a hacker in order to successfully breach your system. These will help develop a strong security plan for your company's defense and enable you to properly recognize the internal environment and identify possible targets for breaches.

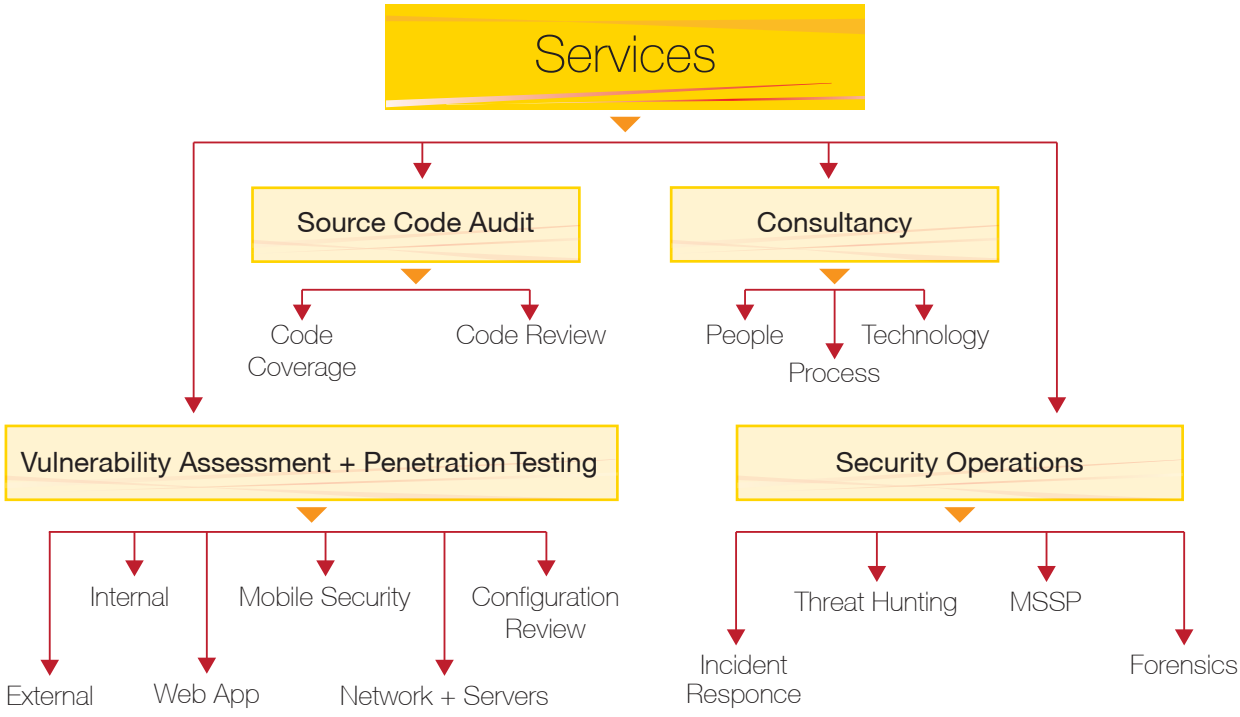
3 Malware Analysis

Through various analysis find out what malwares hackers leave behind after their attack. If unattended, these harmful programs can wake up in a future period and steal information or lock data.

Incident Response

Learn what to do to minimize loss immediately after being attacked

With the state of our digitalized modern world, it is not a question **if** you will get hacked but rather **when** you will get hacked. To know what to do exactly in such an emergency incident, our team will guide you through the steps needed to drastically reduce the damage. One by one we go through the process of preparation, identification, containment, eradication, recovery and report of the incident.

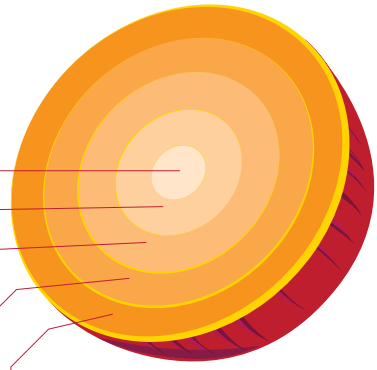


Onion Skin Approach

To maximize efficiency in information security, we recommend an in-depth and comprehensive testing of an entire network structure, especially if that network hasn't been tested in a while.

This comprehensive approach consists of a four-layer chronological method, where our specialized Red Team would start by testing from the outside and gradually make their way into the core or the network, peeling off one layer at a time.

We will assign at least one member of the Beetles Red Team along with an accredited researcher and a CISSP / CISA certified moderator in an attempt to gain access into the system.



Layer 1: Exteranal Penetration Test - The Hacker's Approach

Layer 2: Exteranal Penetration Test - The Known Attacker's Approach

Layer 3: Internal Penetration Test - Behind the Firewall

Layer 4: Network Systems and Confifuration Review

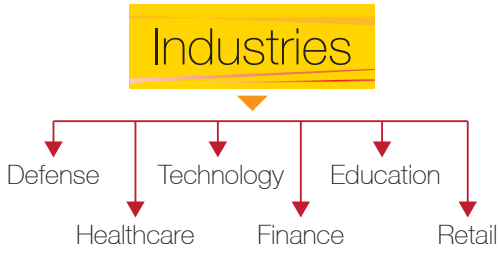
Layer 5: The Core

Our Clients

Ranging from technological to defense sectors our services can be widely applied with satisfying results

Beetles Cyber Security Ltd has been working alongside with some of the biggest brand names domestically as well as internationally. Our client list ranges from large to small scale private companies, major telecoms, the financial sector, digital marketing agencies,

E-Commerce vendors and ITeS companies as well as the government and defense sectors. Truthfully, the services we provide are essential for any organization utilizing the internet in their business processes.



To know more , Please visit: www.beetles.io

The Red Team

Highly Vetted, and Globally Accredited

Beetles has brought together a team of individuals with a broad range of experience who worked both domestically and internationally. Our Red Team consists of the most talented and experienced people in the field of cyber security. They are listed on the fortune 500 tech giant's Hall of Fame, such as Google, Microsoft, Facebook, and are ranked above 100 out of 24,000 in HackerOne™. They have extensive work experience with US DoD, Military and Pentagon on Synack™ and Cobalt™. Alongside them, we share a common vision, to develop the IT security industry in Bangladesh and to raise awareness among the people. All our researchers are under strict Non-Disclosure Agreement Contracts, in accordance with the laws of The Government of the People's Republic of Bangladesh. The team is kept up-to-date with extensive training on the latest technology advances, security adversaries and required skills.

Frequently Asked Questions

Automated scan or manual pentesting?

An automated scan is done using one of the many automated security scanning utilities available to identify vulnerabilities on a wide range of systems in the shortest possible time. It will only test for the most common and well-known vulnerabilities and if the vulnerability does not exist in the database, the scanner will miss it, giving the user a false sense of security. An automated scan is fast, cheap but not accurate.

Manual pentesting is done by leveraging the intelligence, ingenuity and experience of a seasoned, professional security researcher. The security researcher uses their knowledge and experience to manually identify and remove the false positives and to find the false negatives.

An automated scanner cannot think, cannot predict, cannot evolve along with the adversary in an active threat situation and therefore cannot be truly secure; it needs to be combined with the adaptability, creativity and power of the human mind for an optimal security scenario.

A true penetration testing is in taking "The Hacker's Approach!"

What is the difference between the types of services?

A vulnerability scan, is automated and non-exploiting; meaning we will report on detected vulnerabilities but will not attempt to actively exploit these findings. But in a penetration test we will conduct a more thorough, in-depth test that will seek to actively exploit detected vulnerabilities in order to compromise, or set up a scenario where we demonstrate to compromise, your systems and assets just like an outside hacker or attacker would, in a Hacker centric approach to securing your digital domain

What tools do we use?

Our penetration tests are mostly conducted manually because we believe that there is no substitute for the human mind. But even then, we do need the help of some tools to conduct the test more efficiently and thoroughly. Some of the tools that we use are Metaspoilt, Retina, Burp Suite, NMap, Nessus, Openvas etc. But the tool selected for your engagement may vary based on our perception of the appropriate tool necessary to properly assess your requirement and application.

We will consult with your administrative and technical personnel to determine the most effective manner in which to perform the internal vulnerability assessment. Generally, your test can be performed through allowing Beetles a temporary Virtual Private Network (VPN) connection to our internal network. We will make sure that you enable necessary logging and implement practices to ensure our administrative and VPN privileges are disabled after the completion of our testing.

Who will perform the tests?

Your tests will be conducted by our Beetles Red Team, consisting of highly vetted and carefully selected researchers from our global resource pool. All our researchers are regularly evaluated based on their work and client reviews. They are subject to extensive background checks and have confidentiality and non-disclosure agreements with our firm.

What is the time frame for performing a vulnerability test?

We can perform your penetration testing in two to three weeks, in general, after we receive the official work order. If you require an expedited test, we can customize a schedule for you.

How will I receive the finding from the vulnerability assessment?

We issue a formal report for all our review services. This report will include an overview of the findings from our test as well as any recommendations regarding remediation. You will be invited to join our proprietary Beetles – The Hacker's Approach Platform, where you will be kept updated on the current status of your test as well as have access to all your results. Our researcher's every action and movement will be logged and you will be able to monitor our work in real-time. You will receive formal reports of our review services here and the report will include the details of the findings from the test as well as any recommendations regarding remediation. You will also be able to download a PDF copy of your report, if you wish to do so.


SAFETY
Password
Protection
likes
Security
Code
dislik
financial
history
friends
PERSONAL DATA
Data
INFORMATION
Information
Data
Privac
PRIVACY
Security
SAFETY
Protection
Password
FRIENDS AND FAMILIES
financial history
SECURITY
Data
Code
Protection
information
likes and dislikes
PROTECTION
SAFETY
families
Information
Protection
Informatio

BEETLES
THE HACKER'S APPROACH

Aziz Bhaban
93, Motijheel C/A (3rd Floor)
Dhaka-1000, Bangladesh
Phone: +880-2-9513744
E-mail: query@beetles.io
Web: www.beetles.io