ALPHA THREAT

SERVICES

🌐 https://www.alphathreat.in

✉ info@alphathreat.in

☎ +91-9368575559

COPYRIGHT

INDEX

INTRODUCTION 4

ABOUT US 6

SERVICES 7

PENTEST STANDARDS 12

AUDIT METHODOLOGY 13

DELIEVERABLE 14

TESTIMONIAL 15

INTRODUCTION

Cybersecurity in today's world ensures the protection of digital assets and network of an organization from threats in today's cyber space. Cybersecurity issues are becoming a day-to-day struggle for businesses. With the introduction of Bring your own device (BYOD) and Work from home, the security risk have simply multiplied.

Recent research shows that the majority of companies are still exposed to cyberattacks due to lack of cybersecurity practises and unprotected data.

Below are some statistics to consider

- Hackers attack every 39 seconds, on average 2,244 times a day. *(University of Maryland)*
- 62% of businesses experienced phishing and social engineering attacks in 2018. *(Cybint Solutions)*
- Data breaches exposed 4.1 billion records in the first half of 2019. *(RiskBased)*
- By 2020, the estimated number of passwords used by humans and machines worldwide will grow to 300 billion. *(Cybersecurity Media)*
- 34% of data breaches involved internal actors. *(Verizon)*
- 17% of all sensitive files were accessible to all employees. *(Varonis)*

Statistics by Symantec shows that hackers have shifted their focus to small organisations due to lack of security appliances and awareness among employees in large corps.. It is noteworthy that small businesses make up 58% of all cybercrime victims and the average cost of a small business cyber attack is roughly $35k.

60% of small businesses that experience a data breach go out of business within 6 months of the cyber attack as clearly stated by US Securities and Exchange Commision.
90% of all cyber attacks are the result of human error within an organization.

WHAT IS AT RISK

- CLIENT PERSONAL INFORMATION
- CLIENT FINANCIAL INFORMATION
- YOUR BUSINESS'S BANK DETAILS
- YOUR COMPANY REPUTATION
- NORMAL BUSINESS OPERATIONS
- YOUR BUSINESS PLANS OR DESIGNS
- COST OF CLEARING THREATS
- OTHER SENSITIVE PERSONAL OR BUSINESS-RELATED INFORMATION

ABOUT US

Alpha Threat simply aims to be your trusted cybersecurity go-to partner, bringing advanced expertise in modern day threat landscape. We provide cost effective technology to small and medium enterprise thus reducing security risk to minimum. Along with the licensed tools in our arsenal our in-house developed technology and tools helps industries to actively suit their requirements while being cost effective

Digital CyberSecurity Agency

Our unique layered security audit approach helps customers not only to eradicate security vulnerabilities but also to minimize the impact to minimum in case of any attack.

HTTPS://WWW.ALPHATHREAT.IN
INFO@ALPHATHREAT.IN

SERVICES

✓

VULNERABILITY ASSESSMENT

Vulnerability testing helps organizations identify and eradicate vulnerabilities in their software and supporting infrastructure before a compromise can take place. Network Architecture review is also performed based on scope

✓

PENETRATION TESTING

Pentest is performed considering the perspective of an outside attacker or a malicious insider. Pentest also helps an organization remain compliant with leading certifications like PCI, GDPR, etc. Follows PTES, OSINT guidelines

✓

CONFIGURATION/LOG REVIEW

The purpose of the Configuration Review is to verify the operating condition and effectiveness of the security configuration and rulesets of the network and securitiy devices. Follows CIS guidelines

SERVICES

✓ MOBILE APPLICATION AUDIT

Tests for Functionality, Usability, Security, and Performance of mobile applications (ioS/ Android) by static and dynamic analysis. Follows OWASP mobile guidelines

✓ WEB APPLICATION AND SERVICES AUDIT

Audit of website, applications and web services based on globally recognised OWASP standards. Also includes testing for logical and business flaws. Follows OWASP and SANS 25 guidelines

✓ CLOUD SECURITY

While cloud infrastructure comes with builtin security features a lot of them are looked. Cloud security audit includes identification and elimination of threats persisting in your cloud infrastructure

SERVICES

SOURCE CODE REVIEW

Checking the source code of applciations and softwares for underlying vulnerabilities. This test is effective to detect bugs related to Buffer overflow, Encryption issues, Injection, Insecure coding practise, etc

CONFIGURATION HARDENING

This audit aims to find the vulnerabilities in the core of the Operating systems. It includes points related to User managemet, auditing, logging, privilege escalation, running services and a lot more. This test follows CIS guidelines

THREAT INTELLIGENCE

We provide daily feeds to clients about the trending attacks and the malicious IP address. This list can be utilised to feed the firewall and other security devices

SERVICES

ADVERSARY EMULATION

Test for the security and logging capabilities of implemented security controls. Emulation for real APT Tools, Techniques and Procedures (TTP's) under controlled environment

STRESS TESTING

Test for the ISP capability during peak hours. Tests performed by sending heavy traffic on layer 3,4 and 7 of the OSI layer. Know your defenses against DDoS attacks

PHISHING AS A SERVICE

Test your employees ability to identify and defend against phishing attacks. No data leaves the organization

SERVICES

FORENSICS

- Disc forensics
- Mobile forensics
- Password cracking
- OSINT, Social media and Darkweb
- Court preparation and Testimony
- Consultancy for Cyber Forensic lab setup
- Internal fraud investigation
- Academic lab setup
- Forensics training

TRAINING

- Cyber security training for students
- Cyber security awareness training for organization and Law enforcement

DARKNET RESEARCH

Darknet often referred to as **Darkweb ,** simply put is a network of secret websites that can be accessed over an encrypted network. These websites are not indexed by common search engines like Google. This is a marketplace of cyber criminals. A simple Google search of "Darknet database leaks" will reveal the statistics.

Our team of dedicated experts continuously keep an eye out on Darknet and similar marketplaces for such breaches. We found majority of Medium and Large scale corporations had their internal emails exposed with cleartext passwords. Investigating further revealed that most breaches occured simply due to lack of awareness among employees which went unnoticed by their security solutions

Our team covers channels which are a common meeting point of hackers. Our team remain in touch with darknet communities to ensure our client's safety and keep an open eye for any breach. Our team research the darknet and will find if your organization is, or have ever been compromised. We try to collect the source and technique for the breach.

This helps to understand the latest attack methodologies used by the threat vectors, thus keeping us updated, which helps us to provide a proactive approach to mitigate the vulnerabilities at the earliest.

SERVICES

CYBERSECURITY AWARENESS TRAINING

Your employees are the first and primary line of defense against online cyberattacks. Equipping your employees with the training and skills makes them a perfect warrior against cybercrimes

- In the 2019 DBIR, 94% of malware was delivered by email. *(Verizon)*
- In a different sample, 92% of malware is delivered by email. *(CSO Online)*
- 48% of malicious email attachments are office files. *(Symantec)*

With our always up to date training modules, we make sure to provide your employees a real time simulated experience of the threats and their impact. We provide real demo for the attacks with live interaction, thus enhancing the learning experience. We cover major topics on Active threats, Case studies, Attack Methodology, Impact and Identifying & Mitigating threats thus enhacing the overall security posture of your organisation.

PENTEST STANDARDS

Alpha Threat adhere to the below provided standards for the related audit activities

PTES

Penetration Testing Execution Standard provides guidelines to be followed to conduct a successful pentest.

OWASP/ SANS 25

Open Web Application Security Project (OWASP) and SANS 25 defines guidelines to be followed for pentesting of Web applications. OWASP mobile defines standards for pentesting of mobile applications

OSINT

Open Source Intelligence provides methods on collecting vital information from available public sources. Useful in recoinassance phase during a pentest

CIS

Center for Information Security, a non -profit organization that provides guidelines for hardening of network devices and endpoints

NIST

National Institute of Standard and Technology, implements practical cybersecurity and privacy by providing cybersecurity guidelines for various fields

AUDIT METHODOLOGY

SCOPING

- Discussion to set the parameters for the project.
- Understanding project parameters and requirements

RECONNAISSANCE

- Information Gathering (Active/Passive)
- Target selection and Footprinting
- OSINT

ASSESSMENT

- Network, Port and Vulnerability scanning
- Assessment of vulnerable machines and services
- Exploitation, finding level of privilege escalation
- Whitebox / Blackbox testing

REPORTING

- Submission of a detailed report with all findings
- Report includes screenshots with PoC
- Mitigation steps for all found vulnerabilities

DELIVERABLE

At the end of each activity client receives an audit report with all the detailed findings comprising of below technical points:

- Vulnerabilities found
- Critical Vulnerability Exposure ID (CVE-ID)
- Impact of vulnerability
- Screenshot (Proof of concept)
- Mitigation of vulnerabilities based on highest priority first

Below provided is the skeleton of an audit report:

- Executive Summary
- Scope of work
- Summary of findings
- Conclusion
- Assessment Table
- Screenshots

Feel free to contact us for a sample audit report

TESTIMONIALS

WHAT OUR CLIENTS HAVE TO SAY

"Special thanks to the Security Owls for their rigorous support in our cybersecurity audit activity"

Mr. Shivam Singh (Shivnik Solar)

"My data was encrypted due to a Ransomware. Thanks to Security Owls for the timely recovery of files and educating me to prevent further attacks"

Mr. Ashish Kumar (Arc Creation)

"Apart from their technical audit the response and anytime support is very much appreciated. Security
Owls helped us not only to mitigate vulnerabilities but also educate and protect from active attacks"

Mr. Bhupendra Singh (Creative Mojo)

"A malware in my websites affected my online business. Thanks to the Security Owls team for the removal and backing up my business"

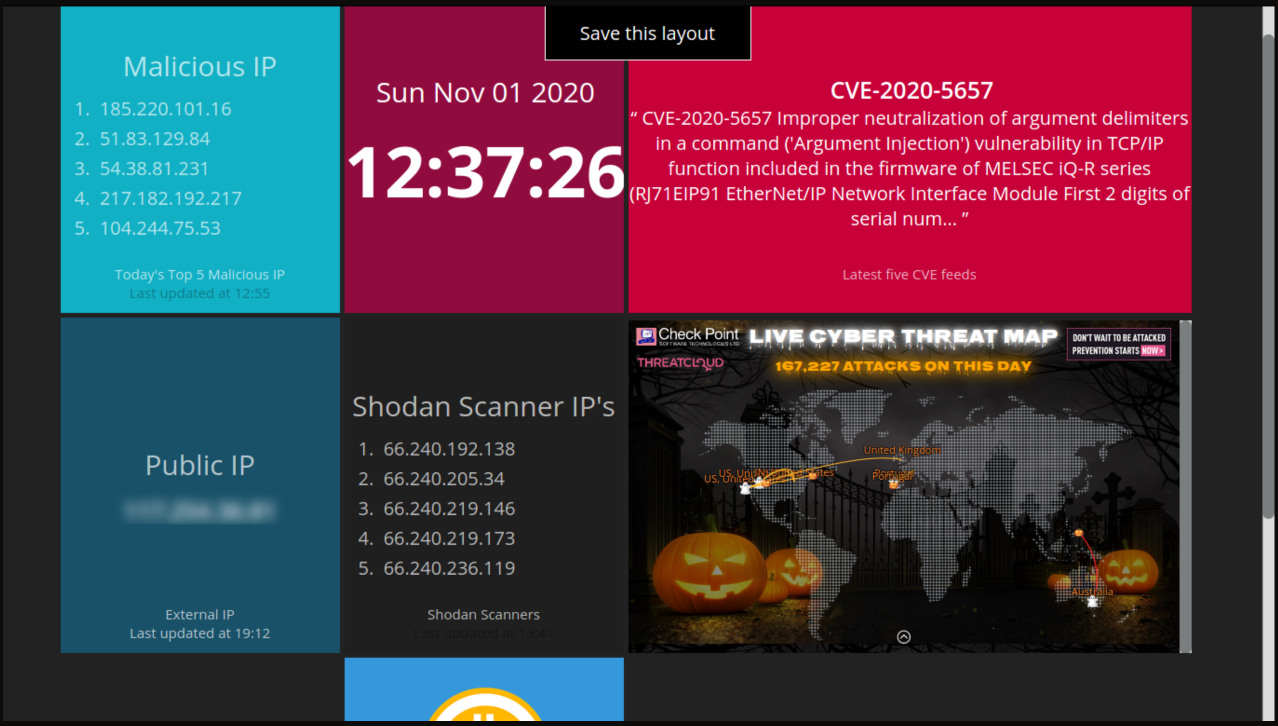
Mr. Ajay Kumar (SchoolModo)

Alpha Threat sincerely cares for its clients and understands the financial limitation of small and medium sector enterprise.

We work continuously to enhance and improvise techniques that could help our clients stay protected. This is why we created an in-house framework that keeps an eye out on Malicious IP addresses and daily active attacks. This framework fetches feeds from various places including Darknet.

The feeds are a collaborative part of our **"Threat Intelligence framework"**

We provide this feed on a daily basis via email to our clients while other companies charge a heavy fees for the same.
This list can be feed to any security appliance like firewall, IDS, IPS, etc to block any originating malicious connection attempt. This technique can effectively block automated attacks originating from internet.



Malicious IP

1. 185.220.101.16
2. 51.83.129.84
3. 54.38.81.231
4. 217.182.192.217
5. 104.244.75.53

Today's Top 5 Malicious IP
Last updated at 12:55

Save this layout

Sun Nov 01 2020

12:37:26

CVE-2020-5657

" CVE-2020-5657 Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial num... "

Latest five CVE feeds

Public IP

[redacted]

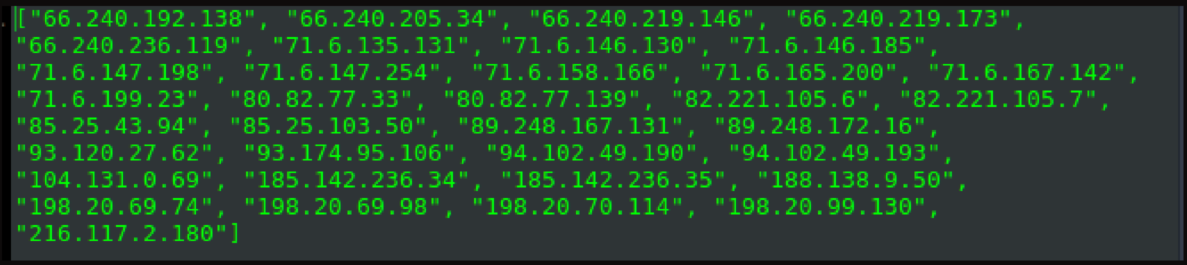
External IP
Last updated at 19:12

Shodan Scanner IP's

1. 66.240.192.138
2. 66.240.205.34
3. 66.240.219.146
4. 66.240.219.173
5. 66.240.236.119

Shodan Scanners
Last updated at 13:41

Glimpse from our Inhouse developed Threat Intelligence dashboard



```
["66.240.192.138", "66.240.205.34", "66.240.219.146", "66.240.219.173",
"66.240.236.119", "71.6.135.131", "71.6.146.130", "71.6.146.185",
"71.6.147.198", "71.6.147.254", "71.6.158.166", "71.6.165.200", "71.6.167.142",
"71.6.199.23", "80.82.77.33", "80.82.77.139", "82.221.105.6", "82.221.105.7",
"85.25.43.94", "85.25.103.50", "89.248.167.131", "89.248.172.16",
"93.120.27.62", "93.174.95.106", "94.102.49.190", "94.102.49.193",
"104.131.0.69", "185.142.236.34", "185.142.236.35", "188.138.9.50",
"198.20.69.74", "198.20.69.98", "198.20.70.114", "198.20.99.130",
"216.117.2.180"]
```

Sample Malicious IP feeds from the framework

CONTACT US

FOR ANY QUERIES

https://www.alphathreat.in

info@alphathreat.in