Company Profile

THREATNIX

We are a tight knit group of experienced security professionals who are committed to providing competent cybersecurity solutions that adhere to international standards. Our team of security experts deliver unbiased guidance and solutions before attacks become disruptions and financial hardships.

We pride ourselves in providing the level of expertise that not only will help the organization identify vulnerabilities and areas of improvement, but also provide guidance on best practices to correct those vulnerabilities.

Mission and Values

Our mission is to bring a paradigm shift in how cybersecurity is strategically and holistically addressed for organizations around the world. We strive to focus all our collective efforts on one single thing - be the first choice for all your cybersecurity needs.

We intend to build a global culture of defending against cybercrime and are confident that our dedication towards it will drive the solutions which will ultimately provide state-of-the-art security for our clients.

Why Us

- [ ] We focus solely on the security concern you need, freeing your internal lead to be able to oversee daily activities to maintain security standards.

- [ ] Our security experts work throughout the year to stay up to date with the latest technology, trends, and best practices in the security industry to provide the best advice and risk-mitigation strategies.

- [ ] Our recommendations are based on your actual needs, not a product or service we represent.

- [ ] We evaluate your business and recommend cost-effective solutions to improve your bottom line.

Our Services

We offer a complete suite of Information Security (IS) related services

including, but not limited to:

IS/IT Audit

IS/IT audit involves a complete assessment of your IT infrastructure that encompasses the policies, procedure, tools, technology, work flow and all other aspects of the infrastructure. It takes an investigative approach to verify that the IT infrastructure is completely secure by examination of evidence and verification of the observed evidence through probing.

Vulnerability Assessment

Vulnerability Assessment helps find out your current security posture. It identifies vulnerabilities and assigns severity levels to vulnerabilities found during assessment. Our assessment method includes Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST).

Penetration Testing

Penetration Testing helps simulate the methods, tactics, techniques and procedures followed by sophisticated attackers. The authorized simulation explores and exploits vulnerabilities before they can be leveraged by malicious entity to cause any damage.

Managed Cyber Security Services

You don't have to worry as all your security needs are fulfilled and managed by your managed cybersecurity solutions partner. Drafting your security policies, setting up your perimeter defence systems, VAPT, compliance monitoring and continuous security monitoring along with security consultations and training are all covered under MCSS.

Security Operations Center

A security operations center continuously monitors your domain and manages your security defences. Don't get buried under the systems' log, network traffic and alerts from your defense systems, let SOC take charge to find the needle in the haystack and strengthen your defense with expert knowledge driven threat detection.

Training and Consultation

Professional consultations on security measures and solutions can provide a clear insight on how to strenghten your security posture. Expert recommendations on tightening your defenses is necessary to ward off attackers. Providing expert training to your personals on cybersecurity is vital to strengthening the human element in security which is identified as the weakest security link.

System Audit and Hardening

System audit ensures that best practices are followed within the implemented system and that the system is on par with the security standards. System hardening addresses any drawbacks that have been encountered in the audit process. System audit and hardening follows a methodical procedure to check for any limitations on security implementations in the system and then manage them properly.

Patch Management

The task of deploying security patches and security updates to systems can be a challenging task, specially if there are large number of systems and there is no set patch management procedure. While patch management addresses the security weaknesses, negligence in the process can result in more severe problems. Proper patch management includes verification of the patches, initial preparation of the systems, application of patch, testing, documentation and cleanup.

Code Review

A software security code review helps to identify and remediate coding errors before they turn into a security risk. When conducted properly, code review can do more to secure your software applications than nearly any other activity.

Incident Response

When a compromising act is detected within your IT domain, it must be handled expertly with extreme caution. Immediately addressing a security incident should be a top priority to keep the damage to a minimum. Incidence response halts the progress of an attack and deals with its management, investigation and recovery.

Site Cleaning and Malware Removal

It is vital to clean a website immediately if any breach or malware infection is detected in your website. With site cleaning and malware removal service malwares, defacement, phishing, injected malicious code, backdoors and spams are removed from your website to get it running smoothly as soon as possible.

Custom Security Tool Development

Security implementations are specific to each individual environment and as such requirement for security tools vary from one organization to another. Generic security tools developed with a broad scope may fail to address your specific needs. So, custom security tools built upon your specific requirements that focuses on addressing your needs will help you implement the best security solution.

Products

i) Asset Management and Discovery System

The asset management system allows administrators to keep track of assets that are active within an organisation's domain. The system compiles a list of IT assets in the network and allows monitoring the assets for anomalous behaviour. The assets and networks can be segregated into groups and monitored comprehensively. Any significant changes on the system can trigger email, notification or SMS alerts. The dashboard gives a top-level centralised view of all the network information collected by the system.
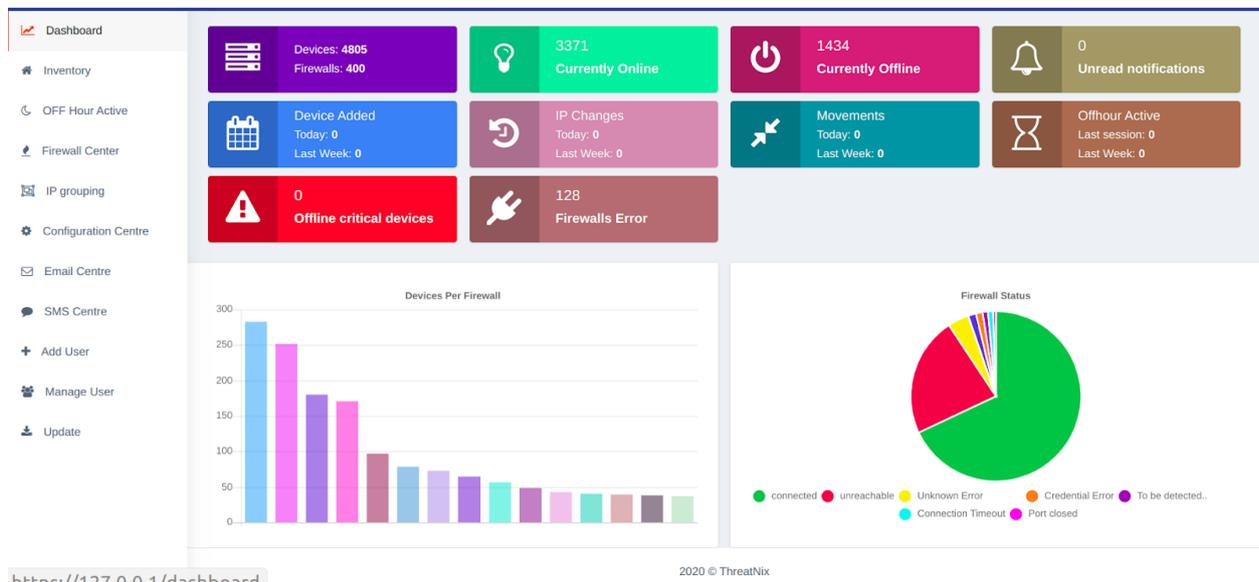
ii) Vulnerability Assessment Tool

Our vulnerability scanner solution features a high-speed vulnerability engine and a feature-rich dashboard to help you identify and monitor security vulnerabilities in both network and applications. The scanner engine comes with an up to date collection of signatures and is intelligent enough to detect technologies in use. The engine only uses relevant POCs to check for potential

vulnerabilities- making it more efficient and fast compared to other known vulnerability scanners while minimizing false positives at the same time.

iii) CSP Monitor

CSP Monitor is a web based application, developed to help implement and monitor Content-Security-Policy (CSP). It allows users to generate CSP policy, evaluates and reports on its strength as well as logs violation reports which are then displayed in a visually pleasing dashboard along with graphs.
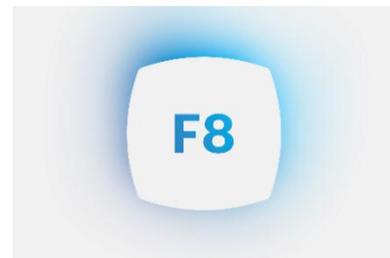
Our Clients

We Have Helped Secure

And many more…

Certifications

Training

Talks

Media Coverage

Public Endeavours

Celebrated Achievements

✓ Research covered by 50+ media worldwide

✓ 1st place in CTF in Blue Hat Shanghai, 2019

✓ Multiple CVEs assigned to vulnerabilities discovered by our team

✓ MVP in Bug Crowd

✓ Top 50 in HackerOne Leaderboard

Contact Us

Threat Nix Private Limited

Kandevta Sthaan 10, Kupondole

Lalitpur, Nepal

📞 +977 01 5448195

✉ info@threatnix.io

🌐 https://threatnix.io