threatSHIELD Security

data security driven by intelligence

SOLUTIONS OVERVIEW

@threatSHIELD Security

PROPRIETARY TOOLS

- *t* INTELLIGENCE (SecurityAppliance)
- *t* MONITORING
- *t* DNS Firewall
- *t* SIEM
- *t* EDR
- PCPAS®

OUR SERVICES

Check our services online, open your phone camera and scan this QR Code!

WHO WE ARE?

- 25 Years exclusively in Cybersecurity
- Active Member of Private Sector FBI
- *11 Years side by side with the FBI
- 8,800+ Reverse Engineering; 8K on APT Malware
- Infra Gard Global Espionage & Intelligence
- CJIS Certification Level 4

"We are on a mission to revolutionize the Cyber Security industry with our innovative model and technology platform"

Felix Negron
Founder CEO

BENEFITS?

- Increases productivity
- Dynamic cybersecurity
- Discovers invisible threats
- Compliment to the firewall
- Increases network bandwidth
- Pro-active detection mechanisms
- Prevents disruption of operations
- Effective and proven detection mechanism
- Monthly report of all detections for compliance
- Alleviates IT overhead – nothing to investigate
- Protects the most vulnerable area of the network
- Shares its intelligence with other security mechanisms
- New intelligence fed every 30 minutes, 24/7 monitoring
- NO human interaction needed - *t* INTELLIGENCE is not a SIEM
- Transfer of intelligence to all security controls on the network
- **Stop** highly malicious cyberattacks before they spread through the network

WHAT MAKES US DIFFERENT?

- 100% Pro-active
- <100% inline solution
- 100% NOT on a mirror port
- 100% pro-active
- 100% detections without human interactions
- <1% false-positives
- Critical data NEVER leaves the network
- Segment-level detection
- Stops in Real-Time all the threats missed by the firewalls and the antivirus; data NEVER leaves the network

OUR SOLUTIONS TSS

Business Maturity Assessment
Ransomware simulation attack
Case Management Platform
Ransomware Remediation
Vulnerability Assessment
Threat Intelligence Feeds
Cybersecurity Education
Compliance Reporting
Reverse Engineering
Monitoring Solution
Cyber Consultation
Incident Response
ZERO Trust Model
VPN Replacement
Risk Assessment
Brand Monitoring
v-CISO Services
v-CISO Compliance
Email Phishing
Network Audit
Forensics
***t* INTELLIGENCE**
***t* DNS Firewall**
***t* Monitoring**
***t* SIEM**
***t* EDR**
PCPAS ®

info@threatshieldsecurity.com | threatshieldsecurity.com | +1 813.291.3693 | 14906 Winding Creek Ct. Ste. 101-D Tampa, FL 33613

Ransomware simulation attack, This is a method by which TSS can test the success or failure of an attack on a company's network. TSS uses a method that is very powerful, with which we can find the weaknesses of the network, discover the areas of concern, and provide the evidence to the client for immediate remediation.

Business Maturity Assessment, A detailed analysis and report of your existing infrastructure's management, security, processes, and performance to identify all opportunities for improvement.

Ransomware Remediation, In the case that your institution is not protected by our 12-step approach and security device, and you are Hit by Ransomware, we perform virus removal, forensics and incident response.

Vulnerability Assessment, Our engineers will identify, quantify, and prioritize the vulnerabilities in your network.

Cybersecurity Education, A well protected network starts with education. We offer Cybersecurity training for your employees on best practices, risk mitigation and password use and complexity.

Threat Intelligence Feeds, Consists of structured data and given context. Access through a URL will be provided.

vCISO Services, We will collaborate with your IT department and perform the same functions as a conventional CISO. The difference. it will cost you a fraction of hiring a full time.

Compliance Reporting, Whether HIPAA, PCI, GDPR, NIST; we've got you covered.

Reverse Engineering, The techniques used by TSS work from five basic perspectives: source, data analysis, presentation, validation, and prediction.

Cyber Consultation, Comprehensive cyber security strategy that prioritizes your investments and stays aligned with security capabilities and strategic imperatives of the organization.

Incident Response, Is a systematic approach to helping IT teams be prepared and plan for IT incidents, including a service interruption, a breach to an organization's security, or a cyberattack.

ZERO Trust Model, threat**SHIELD** Security defeats advanced and sophisticated threats by using an adaptive layered approach. It will use a combination of unique detection mechanisms at the perimeter and local level, creating a powerful distribution of intelligence on all layers of protection.

Risk Assessment, We identify the various information assets that could be affected by a cyber-attack (such as hardware, systems, laptops, customer data, and intellectual property), and the various risks that could affect those assets as well as a prioritizing the risks.

Brand Monitoring, Know the risks associated with your brand, Domain Name monitoring, Internet Monitoring, Marketplace Monitoring, Social Media Monitoring and Logo Monitoring.

Network Audit, We assess compliance! Through our audit we are able to assess whether the company has the proper security mechanisms in place while also making sure they are in compliance with relevant regulations.

Email Phishing, Describes the practice of targeting specific individuals within an organization or business for the purposes of distributing malware or extracting sensitive information. Security awareness and phishing training for employees is a great idea but should not be the only thing they rely on because users make mistakes and are inconsistent.

Forensics, Neutralize threats with intelligent, cutting-edge, investigative and analysis tools. Generating information about Attack context, Infrastructure-wide visibility, Codified expertise, Rich intelligence, Insights.

Pen -Test, We perform a manual simulated cyberattack on your network consisting of 2 hours of reconnaissance, 2 hours of exploits / attacks per IP address and a detailed final report of all findings.

***t* INTELLIGENCE,** Our comprehensive cybersecurity 12-step approach to monitor your network in REAL TIME 24/7 through our proprietary system stopping all attacks before they becomes a breach.

***t* DNS Firewall,** With *t* DNS Firewall enabled, DNS queries for your nameservers get sent to a local threat**SHIELD** Security DNS server where the legitimacy of the requests are checked, and malicious traffic is blocked.

***t* Monitoring,** Is the tool that allows you to measure and improve Operational Efficiency, effectively manager your remote workforce and protect data from insider threats.

***t* SIEM,** (Security Information and Event Management) is a platform that centralizes and analyzes security data to detect and respond to threats, thereby helping organizations manage their security efficiently.

***t* EDR,** Is natively a cloud-delivered solution with full support for on-premises deployments. *t* EDR agents are installed on all your organization's endpoints. Each *t* EDR agent has an event recorder that continuously monitors the endpoint and securely sends insights and suspicious events to the platform.

PCPAS®, Is an advanced cybersecurity system that uses predictive analytics to anticipate potential cyber threats and dynamically adjusts an organization's cybersecurity posture in response. It combines data analysis, machine learning, and cybersecurity best practices to proactively defend against emerging threats.