Technuf

TECHNUF WAY BE CYBERSAFE

#technufcybersafe

Service with Emerging Technology

Cyber Security

- Zero Trust Security Model
- Intrusion detection
- Forensic Analysis and Discovery
- Authentication and Authorization
- Identity and Access Management
- Data Loss Prevention
- Advanced Persistent Threat (APT)
- Counter Intelligence
- User Behavior Analytics (UBA)

Business Intelligence

- Artificial Intelligence (AI)/ Machine Learning (ML)
- Robotics Process Automation (RPA)
- Intuitive Innovative Visualization

Mobile Application Development

- IOS Development
- Android Development
- Business Intelligence Apps
- Multi-platform Support
- Development, Deployment, Operation

Software Engineering and SDLC Automation

- Risk Driven
- Agile
- Industry Best Practices
- CICD/Devops

Our Innovation Center of Excellence Future Proofs our Customer's Technology Path Forward

- Emerging Technology
- Blockchain
- Virtual Desktop Infrastructure
- RPA
- AI/ML

Lessons learned and skills gained from proving advanced initiatives shape our approach to service delivery, provides our customers the opportunity to "plug and play" before they invest and gives our team the environment to offer solutions against a proven environment.

40 W Gude Drive, Suite 220, Rockville, MD 20850 | 301-678-9995 | cybersecurity@technuf.com

IRS | U.S. DEPT OF DEFENSE | NIH NIDDK | FDC | illumina | cisco | DISTRICT OF COLUMBIA PUBLIC SCHOOLS

An uncertain environment can lead to an unprecedented level of attacks!

- 64% of companies worldwide experience cyberattacks.
- Private/Public infrastructures lack strong posture to defend against cyberattacks.
- Cyber criminals attempt access with a range of malware, social engineering and phishing attacks.
- Cyberattacks affect infrastructure, network and confidential data.
- Your first line of defense is a comprehensive, enterprise level cybersecurity plan.

Why do you need to secure your organization?

$4.24 M
Average cost of a data breach

$1.8 M
Average cost of remediating ransomware attack

74%
US Companies experiencing successful phishing attack in 2020

287 days
Average number of days to identify and contain a data breach

Technuf provides secure infrastructure, cybersecurity systems, processes and standards as well as strong frameworks for compliance and governance.

Technuf Four-Tiered Approach

Contact & Exchange

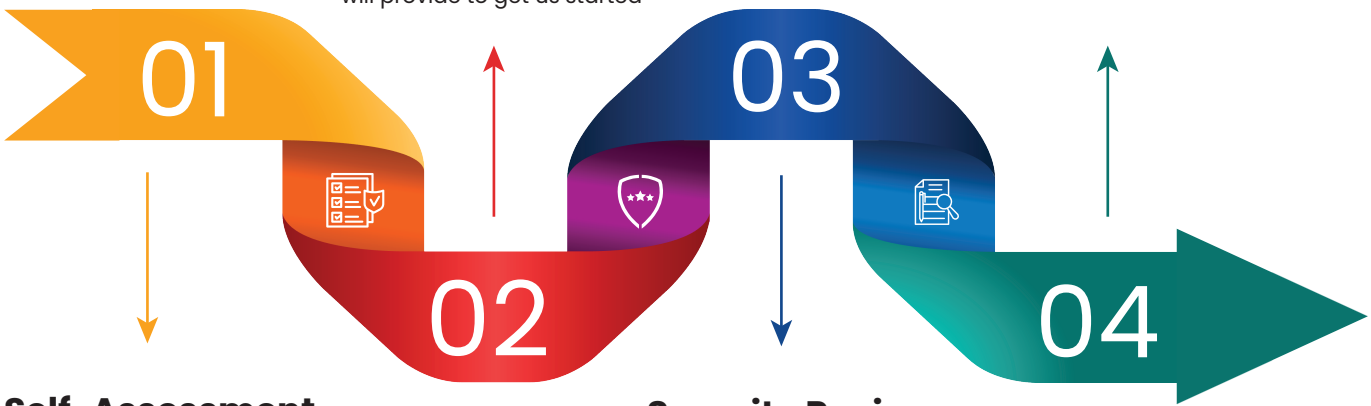
Discuss fine details of your systems and policies with our security experts

Compile a list of necessary documentation your team will provide to get us started

Executive Report

A detailed report including summary of our findings, their causes

Proposed short and long term actions to remediate



Self-Assessment

Online questionnaire to assess your existing security policies

In-person meeting with our security expert to review the responses

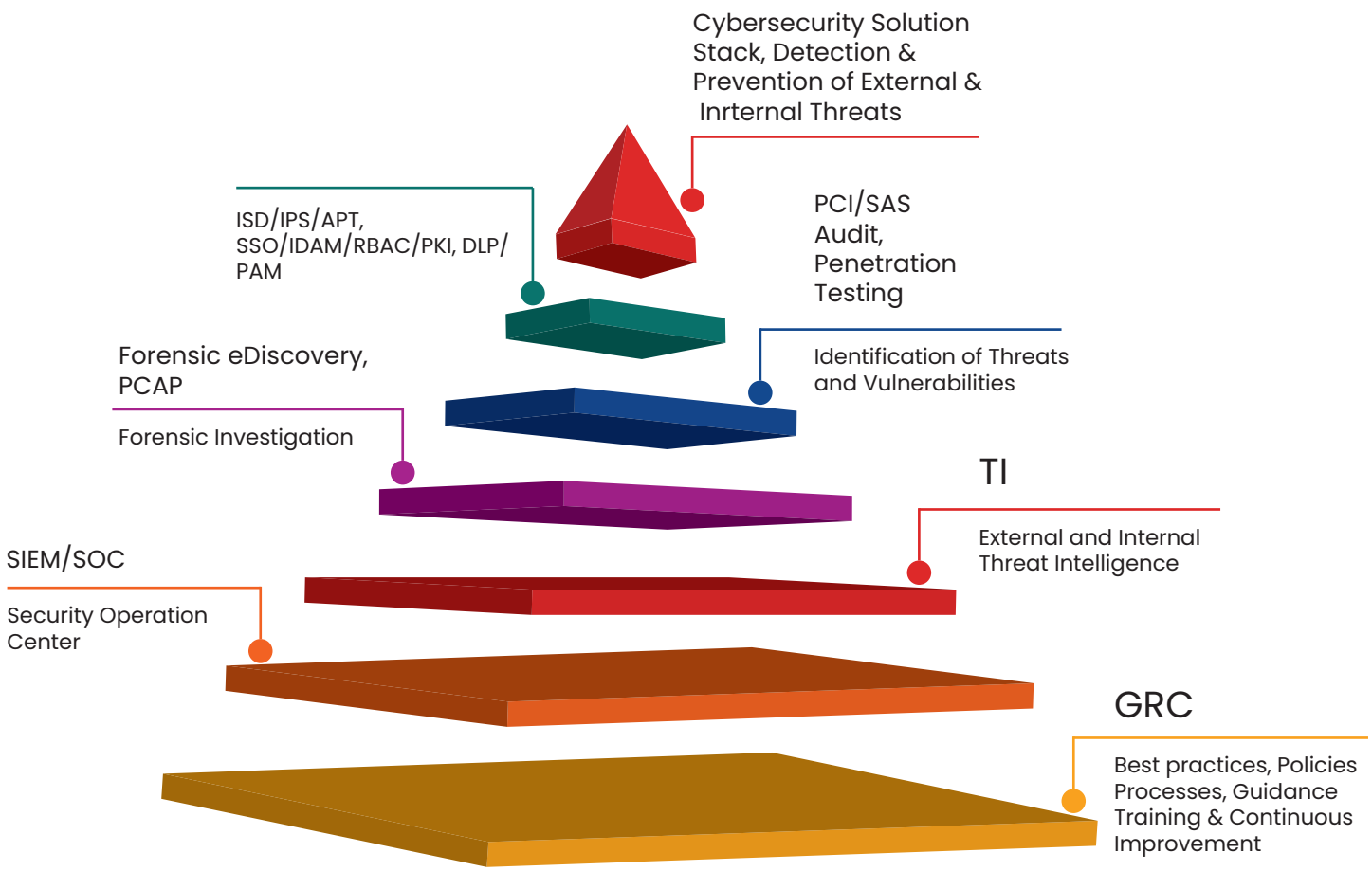
Security Review

Review and analyze the vulnerabilities to determine the root cause

Vulnerabilities are ranked and classified by severity

Technuf

Comprehensive Approach to Cybersecurity



Assessment Requirements

- Main concerns of senior executives
- High-level organizational priorities
- Cybersecurity related policies and processes
- Incident response processes
- Strategic documents
- Known high-risk areas
- Tools already in place

Additional Support

- Support creating/updating cybersecurity policies
- Provide recommendations on cybersecurity tools
- Provide Risk Management support
- Penetration Testing for Web and File Servers
- Vulnerability Scanning for Web and File Servers
- Firewall Configuration and Maintenance
- Remote Endpoint Scanning

Roadmap

The Technuf analyst reviews all collected information and provide a report that shows all findings on the organization's cybersecurity, compliance and over all incident response readiness. The report will highlight all critical elements that need immediate considerations.

- Risks Identified
- Compliance
- Cybersecurity Readiness
- Gaps
- Recommended Roadmap

Technuf

Client Case Study: Security Incident Response

Detect

An employee from an accounting department received a suspicious email from a vendor. Attached was an invoice seeking thousands in payment, however the bank wire details were not the vendor's.

Protect

Our team immediately began enhancing network infrastructure to monitor traffic for unauthorized access to internal accounts and information. This includes procuring and analyzing logs of system access to identify irregular activity, as well as excluding mail flow policies that allowed the attackers to breach user inboxes in the first place.

Respond

Once it because clear that bad actors had compromised employee accounts, they were quickly identified and logged out of all sessions. Each of the mail flow policies created by the perpetrator(s) were removed. Their passwords were reset, and multi-factor authentication was enabled on them as a protective measure.

Root Cause

Business Email Compromise: A bad actor sends a phishing email to obtain account credentials, targets high-value employees through a mail directory, and uses executives' addresses to falsely approve the payment. All messages driving the attack are hidden out of sight in a new folder.

Mitigation & Recovery

Had the attack succeeded, our customer would have given the attackers an unrecoverable, six-figure payment. Long-term mitigation efforts began with a full review and reconfiguration of the organization's connection filter and mail flow policies. Then, we moved to implement a User Awareness Training platform to conduct phishing email exercises. Under our guidance, they have equipped themselves to evade breaches leading to future severe attacks.

Technuf