

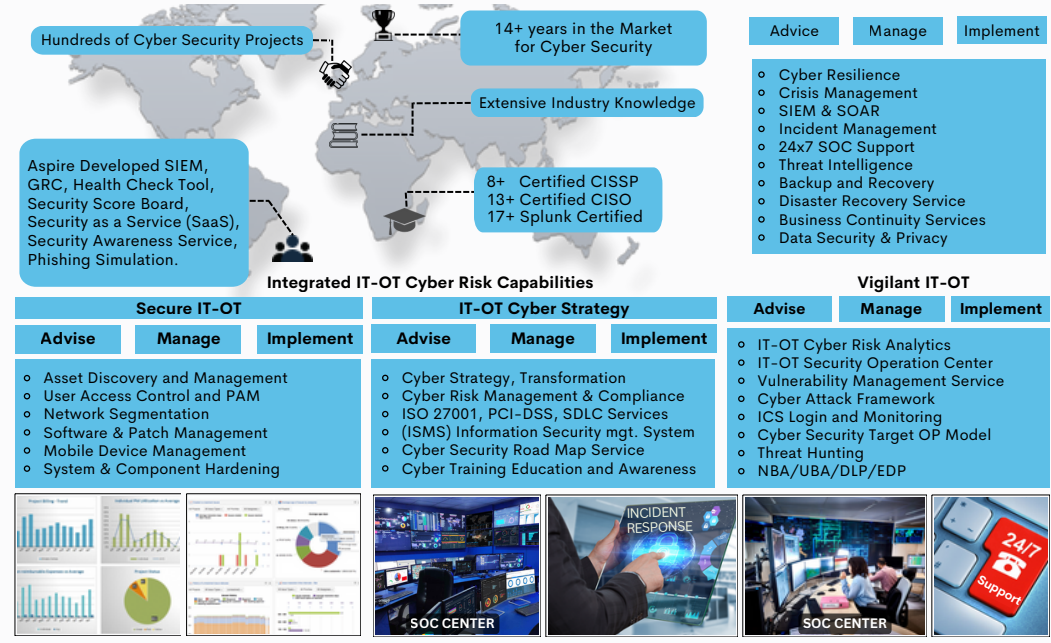


# Aspire Tech Services and Solutions Corporation

# COMPANY BROCHURE

# COMPANY OVERVIEW

Aspire Tech has hundreds of employees in over 13 countries globally.



We have a talented pool of resources spread across USA, EU and Asia.

- ✓ Manage Security Service Provider (MSSP).
- ✓ Global Security Operation Center (G-SOC).
- ✓ Security Architecture & Implementation.
- ✓ Strategy, Governance, Risk, & Compliance.
- ✓ Cyber Forensics and Investigation.
- ✓ Cloud Migration and Integration.

## Tools and Technologies:

- **SIEM:** Splunk, Sentinel, Elastic, A-SIEM.
- **PAM:** CyberArk, BeyondTrust, Delinea.
- **VAPT:** Metasploit, Nexpose, Nessus, Qualys, Invicti.
- **XDR:** Microsoft, SentinelOne, CrowdStrike, Palo Alto.
- **DLP:** Forcepoint, Symantec, Searchinform, CoSoSys.
- **Data Backup:** Veeam, Commvault.
- **Digital Forensic:** Belkasoft, Accessdata, Oxygen, Cellebrite, Magnet, Passware.

## Why Aspire

Aspire Tech has been a top IT Service provider in the Cyber Security, Cloud, and Security Operation Center since 2011.



### A Highly-Experienced Team of Security Experts:

Our teams bring years of extensive experience with domain knowledge and skills in:

- IT security incident management, response handling, and investigation.
- Vulnerability assessment and penetration testing.
- IT security governance, risk assessment, and compliance.



### Leading Certification and Accreditation:

Our security management team has received a multitude of certifications and accreditation including- CCISO, CISSP, GASP, CCSK, CISA, CISM, CRISC, CGEIT, GRCA, GRCP, COBIT, ITIL, CEH, and PMP.



### Regulatory Compliant Processes:

We believe in streamlining our processes against industry-certified methodologies, so you can be assured of the fastest response times and delivery efficiencies with robust security and quality.

- NIST Cybersecurity Framework
- ISO 27001
- ISO 27002
- FedRAMP
- PCI/DSS
- GDPR
- COBIT



### Technology Platform that is both Market-leading and Vendor-neutral:

Our strategic alliances with a rich ecosystem of industry-leading security solution providers ensure that we deliver only the best-in-class solutions available in the marketplace today.



### Cost-Effective and Flexible Implementation:

Choose from flexible deployment options including premise-based, cloud, or hybrid security solutions that best meet your specific security requirements. Gain significant savings with no upfront capital expenditure, while enjoying the flexibility and predictability of a monthly recurring subscription, which lowers the Total Cost of Ownership (TCO).



### International Security Operations Centers:

With 3 international federated Security Operations Centers (SOC) worldwide, our proven security operations provide round-the-clock monitoring and management service. Aligned with ISO27001, ISO9001:2015 CMMI Level 3, CMMI Level 5 and audit-ready.

## Partners



## Our Experts Certified In

CGEIT	CRISC	CISSP	COBITS	CISM	CISA
CASP	CEH	CISCO	Data Protection	SANS Security	CHFI
PMP	PCI DSS	CCSK	GCIH	Network+	ISO
Security+	GSEC	Azure Cloud	AWS Cloud	GCP Cloud	IBM Cloud

## Our Certifications



## Our Top Clients

BASIC Bank Limited	Janata Bank PLC	Bangladesh Police	Special Security Force	Cloud Himalaya	✓ Verizon
Dutch Bangla Bank Ltd	Mutual Trust Bank	BSMR Maritime University	Rajshahi Krishi Unnayan Bank	CCA	IDRA
Midland Bank Ltd	Modhumoti Bank Ltd	Bank Alfalah Bangladesh	Dhaka South City Corporation	CCA	Boeing
				Islamic Bank Bangladesh PLC	

# SECURITY FRAMEWORK

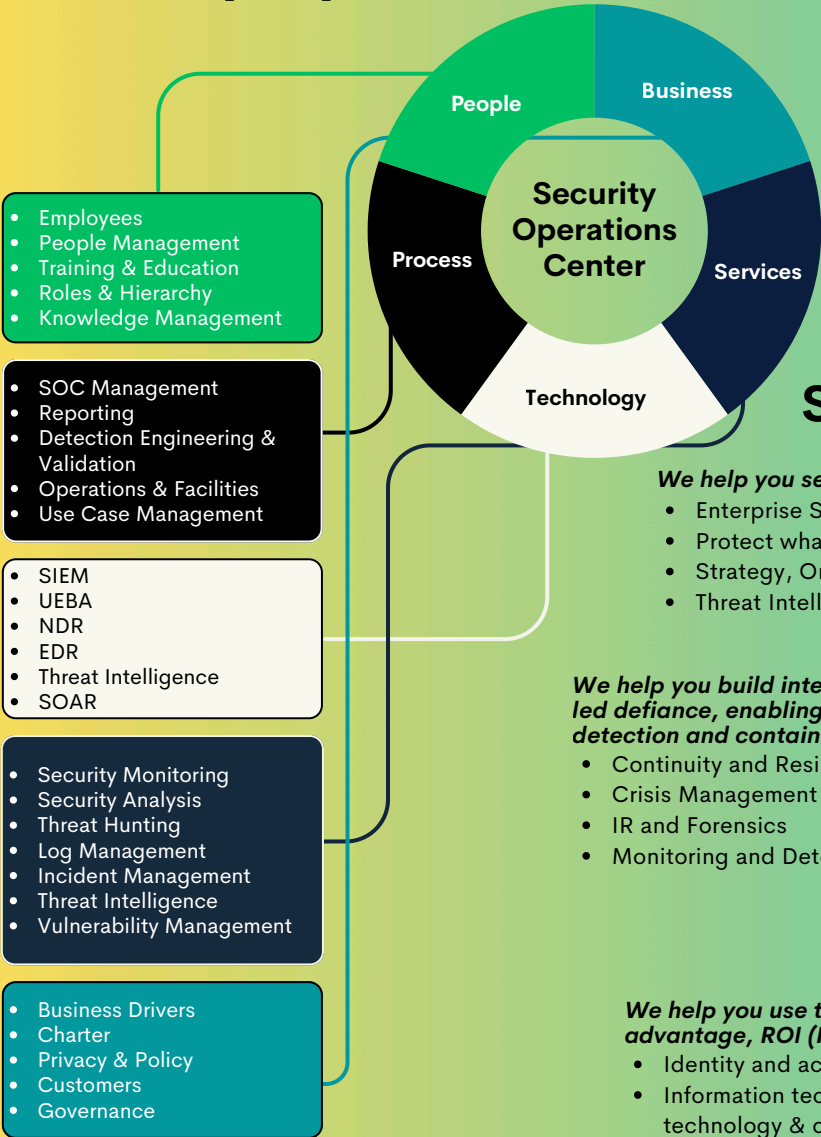


## TODAY'S CHALLENGES

Today's cybersecurity challenges encompass evolving threats like ransomware, supply chain vulnerabilities, and insider risks. Cloud adoption and regulatory compliance further complicate the landscape, while a shortage of skilled professionals and human errors persist. Nation-state actors add geopolitical dimensions. To tackle these issues, proactive threat intelligence, robust defenses, and collaboration are crucial. Adaptation and constant vigilance are essential in staying ahead in the ever-changing world of cybersecurity.



## Security Operations Center



## SECURITY SERVICES WE OFFER:

*We help you set the right priorities*

- Enterprise Security Architecture
- Protect what matters
- Strategy, Organization & Governance
- Threat Intelligence

*We help you build intelligence led defiance, enabling rapid detection and containment.*

- Continuity and Resilience
- Crisis Management
- IR and Forensics
- Monitoring and Detection

*We help you use technology to your advantage, ROI (Return on Investment).*

- Identity and access management
- Information technology, operations technology & consumer technology
- Security intelligence and analysis

*We help you exploit digital opportunities with confidence.*

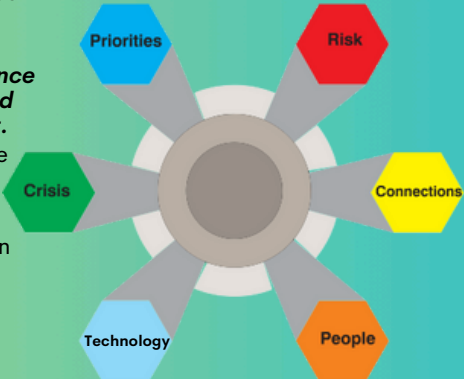
- Digital trust is embedded in the strategy
- Privacy & Cyber Security legal compliance
- Risk Tolerance and Risk Management

*We help you understand & manage risk in your business ecosystem.*

- Digital channels
- Partner and supplier
- Management
- Robust contracts

*We can help you build and maintain a secure culture, where people are aware of their critical security decisions.*

- Insider threat management
- People and 'moments that matter'
- Security culture and awareness



# CLOUD SECURITY SERVICES

## Cloud Security Assessment



- Access and authentication controls
- Client virtual segmentation and compartmentalization
- Hypervisor access controls
- Server security configuration, and build
- Incident reporting and logging
- Incident response planning

## Cloud Security Advisory Services



- Identifying risks,
- Evaluating current controls,
- Identifying gaps or vulnerabilities,
- Making recommendations that are specific to your company's needs.
- Assessing and identifying areas for improvement in your security posture.

## Cloud Protection Services



- Fully managed, enterprise-grade cloud WAF and DDoS solutions
- Organizations benefit from a single pane of glass via a unified portal
- Fully Managed Security Service

## Cloud Security Monitoring



- Identity and Access Management
- Securing Data in the Cloud
- Securing the Operating System
- Protecting the Network Layer
- Managing Security Monitoring, Alerting, Audit Trail, and Incident Response

# WE SUPPORT CLOUD SECURITY TOOLS



## Microsoft Cloud Security Services

- Sentinel (SIEM)
- Defender for Cloud
- Azure XDR
- Advanced Data Security
- Advanced Threat Protection
- Application Gateway Security
- Azure AD Security
- DDOS Protection
- Firewall/Front Door Security
- IoT Security



## AWS Cloud Security Services

- AWS Security Hub-SIEM
- Amazon GuardDuty
- Amazon Inspector
- AWS Shield
- Amazon CloudWatch
- Amazon Macie
- AWS IAM Security
- AWS WAF/VPC
- AWS CloudHSM
- AWS Config/Cloud watch



## GCP Cloud Security Services

- Chronicle SIEM
- Security Command Center
- Event Threat Detection
- Google Cloud Armor
- Web Security Scanner
- VPC Service Controls
- Google Cloud KMS



## Oracle Cloud Security Services

- Database Security Assessment
- Oracle Cloud Guard
- Audit Vault and Database Firewall
- Oracle Data Safe
- Oracle Threat Intelligence
- Oracle Cloud Vulnerability Scanning
- Oracle Cloud WAF

# A-SIEM (Aspire-Security Information & Event Management)

Modern Security Analytics For Everyone!

## KEY BENEFITS

- **Enhanced Security:** Rapid detection and response to cyber threats, safeguarding business data and assets.
- **Regulatory Compliance:** Ensures adherence to data security laws, avoiding legal penalties and fines.
- **Improved Incident Response:** Streamlines the handling of security incidents, minimizing disruptions.
- **Centralized Visibility:** Offers a unified view of security status, aiding in informed strategic decisions.
- **Cost Efficiency:** Reduces long-term security management expenses through automation.
- **Advanced Analytics:** Provides deep insights for better understanding and prevention of security breaches.
- **Performance Monitoring:** Aids in maintaining optimal IT and network performance, ensuring Disaster Recovery (DR) & business continuity.
- **Consumer Trust:** Strengthens customer confidence by demonstrating a commitment to robust data protection.

### Available In

- **APPLIANCE.**
- **VIRTUAL MACHINE.**
- **CLOUD (SAAS).**

## INTEGRATED TECHNOLOGIES IN A-SIEM



Full Packet Capture



MITRE ATTACK



Incident Response



SOAR



Threat Intel



UEBA

## Why Should I Use A-SIEM?

A-SIEM provides ELK as an integrated platform with these additional benefits that do not accompany the ELK Stack itself:



**Easy Deployment**  
Production grade full setup in a hours



**Open Source**  
Avoid vendor lock in by choosing an open source solution



**Alerts**  
Get notified of critical events



**Archiving**  
Store your log files and set your own retention period



**Multi-user & Role-based access**  
Collaborate with your team



**High Availability & Backup**  
Rest that you have the stability of cloud



**Easy Scalability**  
Ship 1 GB to 1 TB of log data each day



**Strict Security**  
Your data is encrypted and is securely stored

### Cloud Security

- Multifactor authentication.
- Monitor out-of-sight assets.
- Identity and Access Management.
- Encryption Standards & Key Handling Tools.
- Cloud Encryption Gateways.
- Mobile Platform Security.

### Incident Response

- Activity Dashboard.
- Alerts/Notifications.
- Behavioral Analytics & Tracking.
- Real-Time Monitoring.
- Collaboration Tools.
- Incident Response.
- PCI Compliance.

### Vulnerability Detection

- Policy Assessment & management.
- Audit Trail & Management.
- Vulnerability Scanning, Threat Response.
- Third Party Integrations.
- Advanced authentication, remediating reports.

### Regulatory Compliance

- Offers predefined report templates that help comply with PCI DSS, GDPR, FISMA, HIPAA, SOX, and GLBA mandates.

### Threat Intelligence

- Deduplication of data.
- Removal of false positives.
- Available APIs and integrations work with existing security tools.
- Data extraction from suspected phishing emails.
- Identify active threats and act fast to resolve threats.
- Compromised Credentials Monitoring & Alerting.

### Endpoint Protection

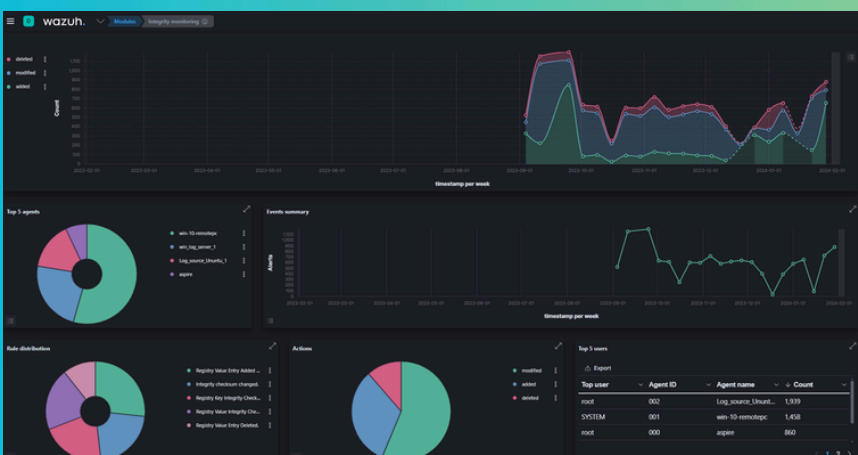
- Threat & Data Loss Protection.
- Device and application control.
- Intelligent alerting and reporting.
- Automated deletion and remediation.
- Behavioral Detection-HIPS.
- Multilayered defense.

## UEBA

- User Account access monitoring.
- Network monitoring, control & analytics.
- Endpoint Detection, Response & prevention.
- Risk scoring & Response orchestration.
- Customizable policies & Risk prioritization.
- Lightweight Agent-Based Protection.
- Leveraging zero-day vulnerabilities.

## SOAR

- Develop and maintain IR playbooks.
- Automate security incident investigations.
- Dynamic case management.
- Create Manual Event, Event Management.
- Custom Functions, Integrate use case.
- Process/Workflow Automation.
- Data Visualization & Monitoring.
- Real Time Analytics, Threat Intelligence.





## Privacy Training

- PCI DSS / HIPAA
- GDPR / SOC 2 / SOX
- CCPA / NY DFS / StateRAMP
- DFARS / FISMA / FINRA
- CMMC / NIST 800-171
- Data Protection / DPO / IRS E-File
- NIST 800-53 / ISO Advisory

## Role Based Training



- Security Awareness for IT Professionals
- Security Awareness for Managers
- Security Awareness for Executives
- Security Awareness for C-Level
- Security Awareness for Executive Board

## 24x7 Support



Phone  
Email  
Chat

## FEATURE PRODUCTS

- Phishing Simulator
- Dark Web Monitoring
- Password Strength Checker
- Campaign Management

## SECURITY AWARENESS TRAINING

**Learn** Cyber Security  
**Protect**

Yourself/Your Organization

# A-SAT

Boosting Your Security IQ



(Aspire-Security Awareness Training)

Aspire Security Awareness Training (A-SAT) is a multilingual Security Awareness Training and Simulated Phishing platform. It delivers training, and phishing simulations through a combined learning path. With each tier, gain access to an additional level of security awareness training. Aspire Tech can successfully engage and educate your users. This helps you reduce the number of successful phishing attacks and malware infections.

## KEY POINTS



User Friendly LMS



3 learning method



148+ Modules



5 Different Languages



Dynamic Reporting System



User Assessment



Role Based Training



Certification



24x7 Supports



Customizable Training Packages

## KEY FEATURES FOR TRAINING



Created by Security Experts.



Access Period: **12 months**



Course Duration: **1+ hours**



Quizzes & Revision Exams:



Multilingual Topics:



Certificate of Completion:



Support: **24/7 hours**



Online  
Bootcamp

## Topics List

Web Video Animation

GDPR	✓	✓	✓
HIPAA	✓	✓	✓
Malware	✓	✓	✓
PCI DSS	✓	✓	✓
Vishing	✓	✓	✓
Smishing	✓	✓	✓
Phishing	✓	✓	✓
Antivirus	✓	✓	✓
CEO Fraud	✓	✓	✓
Ransomware	✓	✓	✓
USB Baiting	✓	✓	✓
Data Security	✓	✓	✓
Email Security	✓	✓	✓
Insider Threat	✓	✓	✓
Physical Security	✓	✓	✓
Security Analytics	✓	✓	✓
Email Safety Alert	✓	✓	✓
Social Engineering	✓	✓	✓
Threats to IoT Devices	✓	✓	✓
Password Management	✓	✓	✓
Removal Media Device	✓	✓	✓
Evil Sides of Dark Web	✓	✓	✓
Safe Internet Browsing	✓	✓	✓
Evil Sites of Dark Web	✓	✓	✓
Safe Wireless Networks	✓	✓	✓
Mobile Devices Security	✓	✓	✓
Remote work from home	✓	✓	✓
BYOD & Mobile Security	✓	✓	✓
VPN working from home	✓	✓	✓
Vishing-Don't be a victim	✓	✓	✓
Links and Files:Click Wisely	✓	✓	✓
Shoulder Surfing (Data Leak)	✓	✓	✓
Report for Stronger Security	✓	✓	✓
Multi-factor Authentication	✓	✓	✓
Push Notifications Unmasked	✓	✓	✓
Safe Disposal of IT Equipment	✓	✓	✓
Protect Yourself-Stop Malware	✓	✓	✓
Cloud Security Threats & Risk	✓	✓	✓
Recognizing Social Media Risks	✓	✓	✓
How to Stay Safe for The Holiday	✓	✓	✓
Threat Identification & Mitigation	✓	✓	✓
Best Practices for Securely QR Codes	✓	✓	✓

# A-SOC

(Aspire-Security Operations Center)

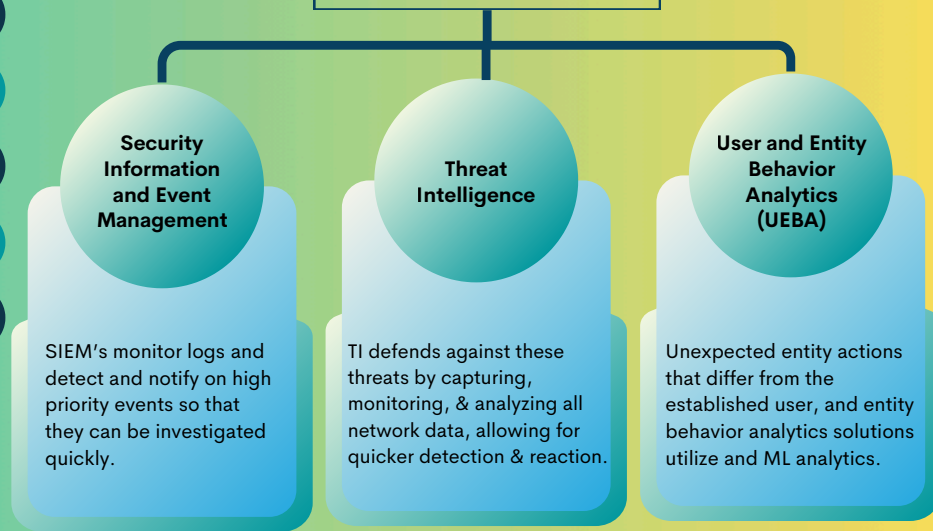
Where Security Begins

Setting up a Security Operations Center (SOC) is now an essential part of any security plan and data protection system aimed at decreasing IT infrastructure threats from both external and internal sources. If you're having trouble keeping your Security Information and Event Management (SIEM) solutions up to date, hiring a 24/7 Security Operations Center and Incident Response team. We are here to help.

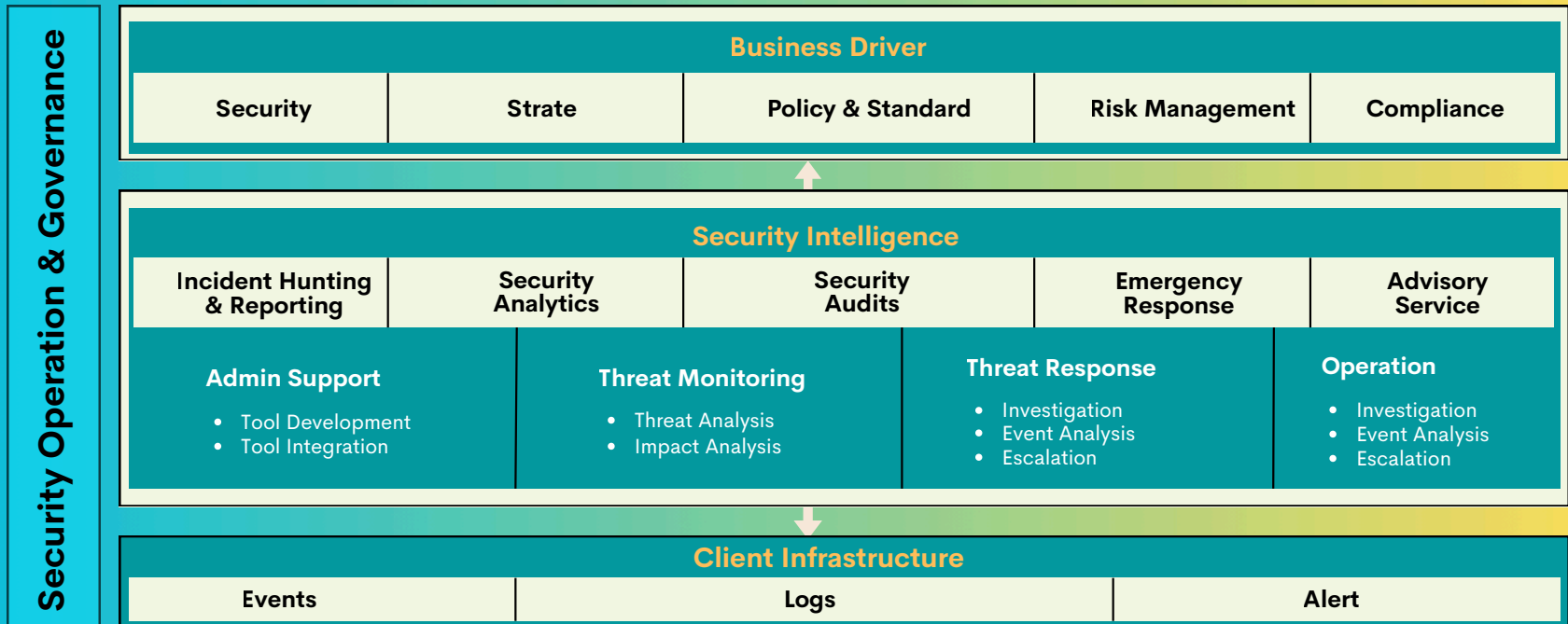
## Key Features



## Increase Context with Data Enrichment



## SOC Framework



## The Key Functional Components of SOC

IT compliance and audit confirm adherence to regulations and security policies, mitigating risks and safeguarding data within an organization's technology environment.

IT compliance and audit confirm adherence to regulations and security policies, mitigating risks and safeguarding data within an organization's technology environment.

Tools and technology encompass software, hardware, and equipment that enhance productivity, streamline processes, and facilitate innovation in various industries and sectors.

Incident management involves promptly identifying, responding to, and resolving disruptive events or issues, minimizing their impact on business operations.

# A-GRC

(Aspire-Governance, Risk, and Compliance)

Your Governance & Compliance Partner



## A-GRC is Specially Designed For

Financial Services

Technology

Health Care

Local Government

Law Enforcement

## Key Features of A-GRC



Governance



Compliance



Customizable Risk Assessment

Email Notification



Simplified Administration



Advanced Search



Risk Access Restriction



Encrypted Database



Risk Mitigation Controls



Dynamic Risk Reports

Import and Export



15 Language Translation



Integration with ITSM Tools



Available in SaaS



Aspire-Security Scorecard (A-SSC) is a question-based report card that assesses an organization's security risk posture and determine its security level.

## KEY FEATURES

Predictive Analytics

Easy to use

Reporting & Statistics

Intuitive User Interface

Compliance Management

## CATEGORY

Security Awareness

Endpoint Protection

Network Security

Governance

Log Management

Data security

Incident Response

Cloud Services

Software & Application Security

# A-SSC

(Aspire-Security Scorecard)



# A-SHC

(Aspire-Security Health Check)

Stay Secure with A-SHC Insights



## A-SHC AS AN ENABLER FOR IMPROVING INFORMATION SECURITY

RESILIENCE

INFORMATION SECURITY ASSESSMENT

SUPPLY CHAIN MANAGEMENT

AWARENESS

RISK ASSESSMENT

SECURITY ARRANGEMENTS

COMPLIANCE

POLICES, STANDARDS AND PROCEDURES



Aspire-Security Health Check (A-SHC) is a questionnaire-based technique for assessing security arrangements that is simple to use. Its purpose is to help users determine the security state of individual environments within their company. It consists of 398 mid-level information security questions, as well as relevant additional material and an area for recording evidential remarks.

A-Phish is a powerful phishing framework that simplifies testing your organization's exposure to phishing. It makes the simulation of real-world phishing attacks dead simple. The idea behind A-Phish is simple – make industry-grade phishing training available to everyone.

## A-PHISH FEATURES

Cross Platform



Unlimited Phishing Campaigns

Random Scheduling



1000+ Email Templates

Cloning Tool



Real-time Results

Full REST API



Interactive UI

150+ Landing Pages



# A-PHISH

(Aspire- PHISH)

Defend Against Phishing with A-PHISH



# vCISO Services

## Benefits of Virtual CISO Services



Cost Effective



Maximizes Security ROI



Extension Of Your Team

## Virtual CISO Services For Small Business

**From zero to secure in weeks—our virtual CISO services**

- Guide you through the complexities of cyber security.
- Prioritize work on areas of greatest risk.
- Maximize your security budget.
- Meet compliance and/or insurance requirements.
- Build trust and confidence with vendors and clients.



### Full-Scale vCISO

- Experienced executive security leader who helps plan, prioritize, and implement solutions.
- Continuously manage risk efficiently to reduce the impact on the business.
- Dedicated assistance with current security needs.
- The position is mostly remote, with the ability to travel on-site for key initiatives or on a regular basis.

01



### Half-Scale vCISO

- Require less leadership support or is in transition as a result of a CISO leaving the company.
- The Half-Scale vCISO provides security and continuing management, allowing the company to continue operating until a full-time CISO can be hired.
- This position is available both on-site and remotely.

02



### On-Demand vCISO

- A trusted executive-level security advisor, and provides ad-hoc support for enterprises.
- The On-Demand vCISO offers advice and recommendations on security activities, continuous management, and contractual security needs affecting corporate operations.

03



# DIGITAL FORENSIC SERVICES

## Digital Evidence Recovery



- Desktop computers
- Laptop
- Cellular phones
- MP3 devices
- Digital cameras and camcorders
- Personal digital assistant devices (PDAs)
- Any storage device that may hold digital media



## Cyber Fraud Investigation

- Facilitating the recovery, analysis, and preservation of the data
- Recovering any deleted or hidden data from any digital devices
- Helping identify a suspect and establishing a motive for a crime
- Ensuring digital evidence integrity

## E-discovery



- Recursive Data Parsing
- Search Index & Interface
- Tagging & Organizing Documents
- Document Viewing Options
- Audio Transcription
- Optical Character Recognition (OCR)
- Email Threading
- Machine Learning
- Data Visualization



## Incident response

- Respond to threats.
- Triage incidents to determine severity.
- Mitigate a threat to prevent further damage.
- Eradicate the threat by eliminating the root cause.
- Restoring production systems.
- Post-mortem and action items to prevent future attacks.

## Data Breach Forensics



- Automated, intuitive workflow
- Supports hard drives and smartphones
- Indexed keyword search
- Deleted file carving
- Timeline analysis for all events
- Email message extraction
- Network-based collaboration



## Aspire Tech Digital Forensic Services

Our Digital Forensic Services collects all data relevant to your research, analyzing it at a deeper forensic level and generating definitive reports. Digital Forensic Services can help you collect and thoroughly analyze the data you need to successfully complete your digital investigation, whether within a corporate environment or in a law enforcement environment.

## SIEM

- Real-Time Log & Data Collection
- Log Correlation & Threat Intelligence
- Real-Time Notification & Alerting
- Prioritization, Analytics & AI
- Reporting & Dashboards

## XDR

- Internal and External Traffic
- Integrated Threat Center
- AI Detection
- Alert and Data Correlation
- Automated Response
- User Interface

## EDR/ MDR

- Improved Visibility
- Proactive Threat Hunting
- Automated Investigation
- Automated Remediation
- Prioritization
- Recovery

## SOC

- Security Monitoring
- Incident Response
- Threat Intelligence
- Vulnerability Scanning
- Compliance Reporting

## VAPT

- Application Assessment and Testing
- System Assessment and Testing
- External/Internal VAPT
- Black/White Box Testing
- Red Team Assessment
- SANS CWE, CVE, And CVSS
- Customized Solutions

## Compliance Services

- PCI DSS / HIPAA
- GDPR / SOC 2 / SOX
- CCPA / NY DFS / StateRAMP
- DFARS / FISMA / FINRA
- CMMC / NIST 800-171
- Data Protection / DPO / IRS E-File
- NIST 800-53 / ISO Advisory

## Dark Web Monitoring

- Identity Theft Prevention Process
- Threat Intelligence
- Threat Hunting
- Faster Incident Response
- Detecting Physical Threats
- Predicting Potential Terrorist Attacks
- Integration into Security Platforms

# MSSP Services



# About Aspire Tech

Aspire Tech is a consulting-oriented company specializing in cybersecurity and cloud technology, focused on the governmental, financial, and private sectors. Our corporate office is located in New York City, and our regional Cyber Security Operation Centers (CSOC) are situated in Wall Street, Manhattan, USA, and Hi-Tech City, Dhaka, Bangladesh. In comparison to other IT companies, we distinguish ourselves by emphasizing services and combining that focus on cost-effectiveness with modern technology. We are on the brink of penetrating a lucrative market in a rapidly growing industry, encompassing the government, financial, and private sectors.

## Get In Touch



## Aspire Tech Services and Solutions Corp.

### Head Office

Cell phone : +1 (646) 445-9610  
Land phone : +1 (212) 500-7710  
info@aspiretss.com  
11 Broadway, Manhattan,  
New York, 10004, USA.

### Global SOC (GSOC)

+1.646.445.9610  
11 Broadway, NY 10004, USA.

### Regional SOC (RSOC)

+88 01971277473  
Hi-Tech City, Gazipur, Bangladesh.

### Bangladesh Office

+88 01758114433  
+88 01711506834  
info@aspiretss.com  
Bangabandhu Hi-Tech City,  
Admin Building, Kaliakair, Gazipur.

### UK Office

+44 7448 527546  
+44 7395 220349  
info@aspiretss.com  
Fortis House, 160 London Rd,  
Barking IG11 888, London, UK.

### Turkey Office

+90 552 745 31 79  
info@aspiretss.com  
Akcalar Mahallesi, Atatürk  
Caddesi, No 32, Blok D,  
Daire 14 Nilüfer Bursa, Turkey.

### Germany Office

+49 1634470827  
info@aspiretss.com  
Im Hoflehen 13,78098 Triberg im  
Schwarzwald, Germany.

### Singapore Office

+1.917.600.9233  
info@aspiretss.com  
230 Victoria Street, Level 15,  
Bugis Junction Towers, Singapore.

### Brazil Office

+55.119 5943-2816  
info@aspiretss.com  
Sao Paulo, Ez Tower - Morumbi  
- Nova Chucri Zaidan, São Paulo  
-SP, 04711-905, Brazil.

### Gambia Office

+22 07905441  
info@aspiretss.com  
The Disruptive Lab 78 Atlantic  
Boulevard, Bakau, The Gambia.

### Nepal Office

+977.985.101.4046  
info@aspiretss.com  
Central Business Park Thapathali,  
4th Floor, Kathmandu 44600, Nepal.

### India Office

+91 97899 73393  
info@aspiretss.com  
62/66, N Mada St, Tiruvottiyur,  
Chennai, Tamil Nadu 600019, India.

### Philippines Office

+63.968.880.0596  
info@aspiretss.com  
6th, Eastwood Cyberpark,  
CyberOne, 12 Eastwood, Manila,  
Philippines.