FalconEye
Cyber Security

Supreme excellence consists of breaking the enemy's resistance

www.falconeyecybersecurity.com

"Data is the heart of your digital life; keep it beating."

FalconEye
Cyber Security

About Falcon Eye Cybersecurity

FalconEye
Cyber Security

- **Founded, In 2021**
- **3+ Years in Business**

- **Customers across Fortune Enterprises, SMBs, Defence and Government.**
- **50 + Consultants and Growing**

- **Industry Focus** (Banking and Financial, Insurance, Real Estate/Construction, Defence & Government, Manufacturing and Logistics, Retail)

- **Global Presence** (| UAE | India | USA)

- **Partnerships & Accolades**

IBM
tenable
BOLD
Hive Pro
CYBLE
REDSEAL
Cellebrite
cybereason

About Falcon Eye:

Falcon Eye Cyber Security is a significant player in the field of cybersecurity and contributes to enhancing security and resilience by providing cutting-edge solutions and expertise. We offer a comprehensive suite of services to protect organizations from cyber threats, including compliance, threat management, evidence analysis, and SOC operations.

Our Services

SOC

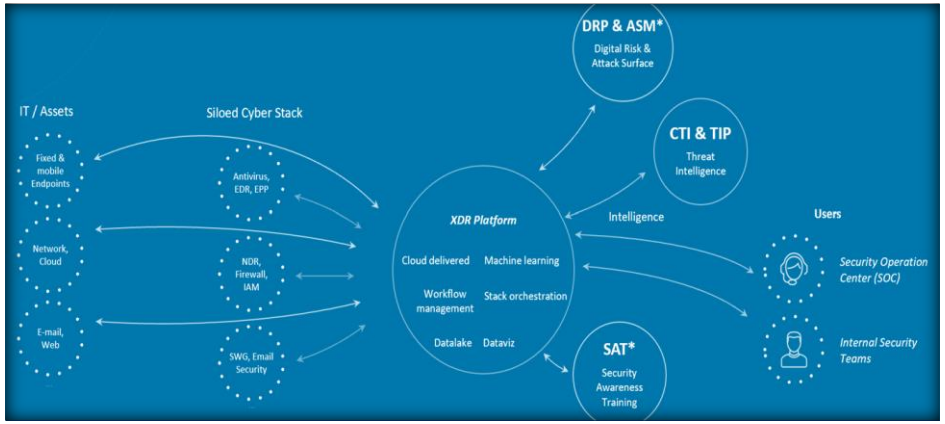
Security Operation Center

Why SOC:

SOC provides continuous monitoring 24/7/365 days of all your infrastructure ensuring the security and resilience of an organization's digital assets from malicious actors.

Benefits of Falcon Eye SOC

- 100 % UAE Presence
- Complete Data Stored on Azure
- Continuous VA & PT
- Integrated Cyber Threat Intelligence 400+ Sources
- Asset-based pricing. MoM billing tends to stay constant



Compliant to Proposed Local Data Residency Requirement

GRC

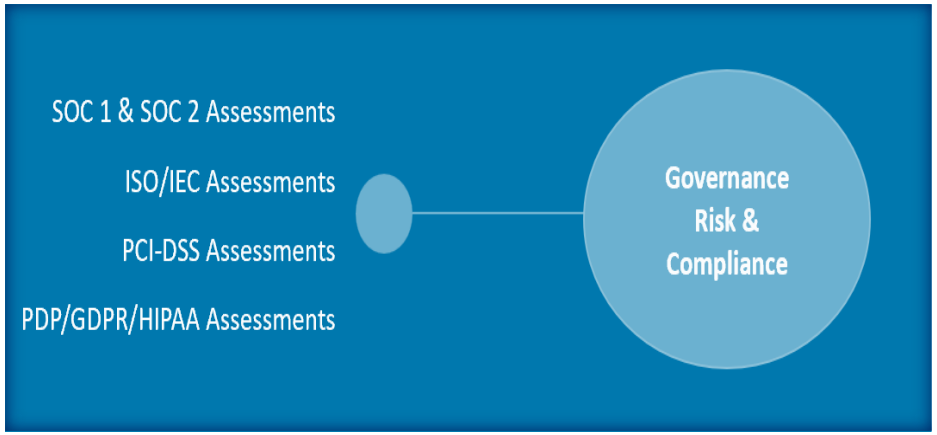
Governance Risk & Compliance

Why GRC:

GRC plays a critical role in cybersecurity. It ensures appropriate governance is in place, cybersecurity risks are properly managed and your organization acts in compliance with relevant laws.

Benefits of GRC

- Increased organization's credibility and cyber resilience
- It enhanced customer confidence
- GRC provides resolution to immediate and long-term risk exposure
- It helps organizations meet country compliance laws



Cyber Forensic Services

Digital Evidence Analysis

Why Digital Evidence:

It is to validate the financial fraud in a court of law.

Cyber forensic evidence tools authenticate the evidence in structure format for ease of analysis.

Benefits:

- Preservation of evidence
- Identification of criminal intent
- Protection of corporate interests
- Assisting in cybercrime investigations
- Facilitating legal proceedings

Forensics Analysis Workstation

Why Forensics Analysis

Forensics analysis plays a critical role in protecting the digital infrastructure and assets of organizations and individuals, helping to prevent financial losses, reputational damage and legal liabilities.

Benefits:

- It protects and safeguards the integrity of the system
- It collects substantial evidence
- It's useful for data recovery
- It protects data and saves money
- It helps to facilitate investigations

Other Services

FalconEye Cyber Security

GRC

- ISO/IEC Assessments
- ISO 27001:2022 (ISMS)
- ISO 22301:2019 - Business Continuity
- PCI- DSS Assessments
- PDPL (Personal Data Protection Law)/GDPR Assessments

Endpoint Protection

- Mobile Device Management (MDM)
- Anti-Virus / Endpoint Protection (EPP)
- Endpoint Detection & Response (EDR)
- Patch Management
- Email Security Gateway

Identity Protection & Governance

- Privilege Access Management (PAM)
- Multi-Factor Authentication (MFA)
- Single Sign-On (SSO)
- IT Service Management (ITSM)
- Identity & Access Management (IAM)

SOC- MSSP

- 100 % UAE Presence
- Complete Data Stored on Azure within the UAE
- Continuous VA & PT
- Integrated Cyber Threat Intelligence 400+ Sources
- Asset-based pricing. MoM billing tends to stay constant

Network Protection

- Perimeter Firewall/ Core /Datacenter firewall
- Web Application Firewall (WAF)
- Distribution Switches/Core Switches/ Other Switches
- Secure Web Gateway (SWG) / Proxy for Content Filtering
- Load Balancer (LB)
- Network Access Control (NAC)
- Network Detection & Response (NDR)
- Network Performance Monitoring (NPM) & Application Performance Monitoring (APM

Cybersecurity Training & Awareness

- We train all users with access to IT – on what NOT TO DO
- Audio & Video Training
- We train how to avoid clicking on potentially malicious links

Risk & Monitoring

- Threat Intelligence & Brand Protection (DRP & ASM)
- File Integrity & Compliance Monitoring (FIM)
- Database Access Monitoring (DAM)
- VA & PT

Data Protection

- Disaster Recovery Backup & Testing
- Backup Solution
- Data Classification (DC)
- Data Leak Prevention (DLP)
- Digital Rights Management (DRM)
- Cloud Access Security Broker (CASB)

Professional Services

- Skill Augmentation
- Niche Skilling
- Building extended team/Offshoring
- Managed Security Professional

Our Products

❑ CyberRiskGuard PRO

- A Streamlined and Quantitative Alternative to Traditional Models
- An AI-Based Approach, that Analyzes 9 Different Risk Parameters, all Identified Risks are Quantified
- Provides “Actionable Intelligence” for Decision-Making
- Risk Quantification
- Accept / Transfer Risks
- Timely Risk Reviews/Analysis & Dashboards
- Risk Performance VS Risk Appetite

❑ SmartComply

- Comprehensive Compliance Management
- All Selected Controls are Broken Down into a Work Breakdown Structure
- All Tasks are Assigned to Specific Personnel
- Dashboards Include Qualitative and Quantitative Performance of each Task and Overall Compliance with Standards

Use Cases - 2

The Customer has been one of the leading multinational fast food retail chains since 1940, offering Big Meal, Chicken Meal, Big Tasty Meal, Royale Meals & many more.

The client operates over 200 outlets across the UAE. There is a significant dependency on IT and Information Systems for Operations across the restaurant, Delivery Services, and back-office ops & analytics.

Case Study- InfoSec

Challenges -

1. We prepare the organization for an independent accreditation along the lines of ISO 27001 – the de facto industry standard for demonstrated conformance to the protection of data within the organization's IT landscape.

2. The standards in scope are ISO 22301 (IT / Business Continuity Management System), and ISO 27001 (Information Security Management System)

Our Solution -

1. The Falcon Eye team is onboarded as a GRC Consulting and Implementation partner for the customer.
2. We helped the customer to implement through the development and deployment of an ISMS (Information Security Management System), Business Continuity Management System & PDPL
3. We set policies, and define and implement procedures supported by guidelines and templates for effective and efficient management of security and privacy across the digital landscape.
4. We provide training through the rank and file of the organization for optimum protection of data.
5. During the InfoSec journey, we established VAPT practice and network modeling to visualize access paths and risk-scoring platforms by using our partner OEM products i.e tenable REDSEAL

Business Benefits-

- Increased Efficiency and Productivity
- Enhanced customer confidence
- Improved information security structure and focus
- Increased organization's credibility and cyber resilience

Use Cases - 3

Customer is one of the UAE's largest diversified automotive dealerships in UAE and is the authorized exclusive distributor of premium cars across the Middle East.

They were using a variety of security tools, and those tools often do not communicate well with each other. This lack of integrations can make it difficult to correlate information and respond to threats effectively.

Case Study- Security Operation Centre (SOC)

Challenges -

1. Before our managed SOC, we find too many false negative alerts and gaps in the existing security tools that fail to detect a genuine threat or malicious activity.
2. The scope requires skilled security teams who can effectively understand and respond to security incidents.
3. We find a lack of automation which leads to slower response times and increases the risk of security incidents.

Our Solution -

Falcon Eye team is the MSSP (Managed Security Service Provider) for the customer.

1. **Threat Intelligence Enrichment**: We automate the enrichment of security alerts with threat intelligence data.
2. **Incident Triage and Prioritization**: Automatically categorize and prioritize incidents based on severity.
3. **Phishing Detection and Response**: Rapidly identify and respond to phishing attacks.
4. **24x7 Monitoring:** We are monitoring 24x7 / 365 days, to provide continuous protection in order to minimize cyber risk to the clients.
5. **Automated Playbooks:** Execute predefined response actions for common incidents.

Business Benefits-

- Centralized Visibility
- Reduced Cybersecurity Costs
- Continuous Monitoring
- Faster Detection and Remediation of Threats

Use Cases - 1

Customer is one of the fastest-growing private wealth management firms in UAE, offering bespoke private wealth solutions and strategies to New Age Entrepreneurs, Business Owners/Promoters, Family Offices, C-suites, and Corporate Treasuries.

They faced a critical cybersecurity threat. Their systems were infiltrated by a sophisticated ransomware strain that encrypted critical databases containing sensitive customer information, transaction records, and financial data.

Case Study- Foiling a Sophisticated Ransomware Attack

Challenges -

1.Rapid Response: The attack had paralyzed essential operations, jeopardizing customer trust and financial stability.

2. Negotiating with Cybercriminals: The attackers demanded a hefty ransom in cryptocurrency for decryption keys.

3.Minimizing Impact: The client needed to restore services swiftly while ensuring data integrity.

Our Solution -

Falcon Eye Cyber Security was engaged to mitigate the crisis:

1.Incident Response Team Activation:

- Falcon Eye's elite incident response team swiftly mobilized, working around the clock.
- They isolated affected systems, preventing lateral movement of the malware.

2.Forensic Analysis and Threat Intelligence:

- Deep analysis revealed the ransomware variant and its propagation vectors.
- Threat intelligence identified the attackers' infrastructure and tactics.

3.Decryption and Recovery:

- Falcon Eye collaborated with law enforcement agencies to track the attackers.
- Simultaneously, they decrypted critical data using advanced techniques.
- Backups were restored, minimizing downtime.

4. Enhanced Security Measures:

- Falcon Eye implemented robust security controls, including:
  - Endpoint detection and response (EDR) solutions.
  - Regular vulnerability assessments.
  - Employee training on phishing awareness.

Business Benefits-

1.Full Recovery: The client regained access to their systems.

2.Improved Resilience: Falcon Eye's recommendations bolstered their security posture.

3.Public Trust Restored: Transparent communication with customers ensured trust.

Thank you

www.falconeyecybersecurity.com

info@falconeyecybersecurity.com

Chandan Ahuja
Director
Falcon Eye Cyber Security
M +971508558429
chandan@falconeyecybersecurity.com
www.falconeyecybersecurity.com