Securing Your Enterprise Assets with Robust CyberSecurity Solution

The increased use of internet for remote business applications, online data sharing, and collaboration presents more opportunities for data loss and theft. We carry much more data and personal information on our mobile devices while we transact on the internet. When a business is connected to the internet in any way, it needs to achieve some level of CyberSecurity. Increasing use of technology also makes firms more vulnerable. This makes CyberSecurity a real necessity for today’s organizations.

At Coforge, our CyberSecurity practice engages with customers in developing strategies to counter various types of cyber threats. We create solutions to strengthen IT security of the organization and meet their specific requirements. We provide an integrated security solution to achieve a cohesive security environment, leverage current investment in tools, and optimize data sources while providing real-time preventive and detective response capabilities for enhanced effectiveness of IT security.

SOLUTION FEATURES

The key features of the offering are:
- Integrated Cyber Intelligence Center (CIC) build-up using intelligent discovery with current state analysis
- Security and compliance using standards and controls
- Multi-tenancy and centralized management
- Centralized vulnerability management of all IT towers through cyber threat intelligence feeds and correlation of events
- Centralized management of IT and IT security devices

The key benefits of the offering are:
- 24X7 continuous and intelligent monitoring: CIC provides real-time monitoring of logs and other system data to quickly formulate a response and mitigate the attack.
- Speed of response: Our analysts are equipped to respond swiftly to malware that has the ability to spread quickly, infecting IT systems and encrypting, exfiltration, or otherwise damaging data in mere seconds.
- Intelligent analysis: Our CyberSecurity technology helps incident responders with the ability to analyze the incident after it has happened to defend against future attacks. The CIC is also enabled with the cyber threat intelligence feeds to intelligently analyze potential security threats.
- Automated remediation and recovery: The offering helps clients recover from or stop DDoS attacks, data exfiltration from insiders and other threats in a reasonable amount of time.
- Centralized reporting: Our dashboards keep executives, auditors, and security personnel apprised of all security issues or incidents. The centralized reporting also generates compliance reports for various security standards.
OUR OFFERINGS IN CYBERSECURITY DOMAIN ARE:

1. Threat and Vulnerability Management
2. Security Controls and Identity Management
3. Security Crisis and Incident Response

1. Threat and Vulnerability Management
Vulnerability assessment supports the discovery of vulnerabilities in existing systems, subsequent decisions and remedial actions, e.g. software patches. This assessment service determines the nature of security vulnerabilities, which exist on the network as well as hosts, and methods of mitigation. The assessment covers network equipment like routers, switches, firewalls etc. and operating systems like Windows NT, Solaris, and Linux. This activity is usually performed by executing tool-based scans on network and hosts within the client’s internal network.

The offering encompasses the following:
- Threat Detection: Actively identifying and isolating threats to minimize their impact upon assets
- Vulnerability Detection: Actively identifying asset weaknesses before they can be exploited by an attack
- Threat and Vulnerability Remediation: Isolating and resolving asset security issues once identified
- Security Information Management: Integrating, interpreting, and presenting security-related information from disparate sources

2. Security Controls and Identity Management
Security and Identity Management level includes identifying desirable system controls as defined and documented by the client. This is followed by reviewing implemented system controls by conducting a comprehensive audit of current information systems, identifying controls implemented, and evaluating effectiveness and completeness of control. This is followed by a gap analysis of the controls, which comprises identifying gaps in the controls implemented and the potential weaknesses.

Finally recommendations and solutions are presented for improvement and enhancement of the system controls. This essentially involves the following two methods:
- Business Process Controls and Compliance Management
  - Objective: Identify and agree on control objectives
  - Control Definition: Define system and application controls to be implemented
  - Control Risks: Identify and assess potential risks in the absence of controls
  - Control Techniques: Define methods of implementing controls

3. Security Crisis and Incident Response
This involves conducting a comprehensive review of the three core components. The objective is to determine the adequacy of the crisis and incident response techniques defined. The three core components are:
- Application Security: Under this core applications are examined and existing processes are reviewed to formalize administration and crisis response mechanisms.
- Network Security: Network infrastructure and configuration management techniques are reviewed for integrity. Incident handling and response mechanisms is defined for the core infrastructure.
- User-Level Security: Existing policies and recent incidents are reviewed along with current best practices to define an appropriate user-level security framework.

3. Security Crisis and Incident Response also includes the following three activities:
- Incident Monitoring and Handling
  - Investigation Management: Defining the management model for security investigations
  - Emergency Responses: Defining the response during various types of emergencies
  - Root Cause Analysis: Identifying the root cause of an incident

THE COFORGE ADVANTAGE
- Complete adherence to required standards such as ISO, PCI/DSS, SOX etc. and security compliance
- Access to a single version of truth for IT and IT security health through a centralized dashboard
- Total cost of ownership reduction
- Better prevention and remediation through analytics
- Continuous innovation driven automation first approach
- A security solution that incorporates enhanced flexibility and agility
- Global security solution enabled 24X7 security monitoring
- Predictive deliverables in alignment with business outcomes and expectations

- Emergency Response Planning
  - Response Team Coordination: Defining the coordination mechanism between the teams, i.e. escalation lists and responsibilities
  - Policy and Procedure Development: Developing suitable policies and procedures
  - Response Plan Testing: Testing the response plan for practicality and effectiveness

Electronic discovery
- Forensic Analysis: Defining an outline to conduct forensic analysis
- Evidence Handling: Defining a method to handle evidence
- Litigation Support: Preparing evidence for litigation purposes, such as disciplinary action
Coforge is a leading global IT solutions and services organization which believes that real transformation cannot be driven by thinking in technology terms alone. With a mission to “Transform at the Intersect” it aims to bring both deep domain and deep emerging technologies expertise to achieve real-world business impact. A focus on very select industries, a detailed understanding of the underlying processes of those industries and partnerships with leading platforms provides us a distinct vantage. We leverage AI, Cloud and Insight driven technologies, allied with our industry expertise, to transform client businesses into intelligent, high growth enterprises.

Learn more about Coforge at: www.coforgetech.com

Stay connected: