Cyber Security Strategy by Industry

Best Practices for Defenders

SMALL AND MIDSIZE BUSINESS

- Mandatory corporate cyber security policies and education for all staff.
- Encrypt everything securing all records and confidential data.
- Use firewalls and anti-virus software that includes virtual private network (VPN) support, anti-virus, anti-spam, anti-spyware, and content filtering capabilities.

ENTERPRISE

- Real-time network visibility, it is key to understand what normal looks like on the network, so abnormal activity can be pinpointed earlier and quicker.
- Comprehensive threat detection and mitigation, so that threats like Botnets, DDoS and Malware can been seen and then blocked.
- Rapid incident management and tools that provide detailed forensics for compliance.

EDUCATION

- Overarching cyber security policies and visibility of all devices and users on the network.
- Quick troubleshooting tools, so network issues e.g. configuration issues and security incidents can be diagnosed and then triaged rapidly.
- Bandwidth monitoring and capacity planning.

PUBLIC SECTOR

- Appropriate cyber security management policies and processes, communicated to all staff.
- Manage and monitor users who access sensitive information/ key operational services.
- Implement an incident response and management plan, with clearly defined actions, roles and responsibilities.

telesoft

DATA CENTER

- Employ tools that identify applications regardless of port, protocol, or evasive technique, including the decryption of encrypted traffic.
- Identify and control users regardless of IP address, location or device.
- Detect and block known and unknown application-borne threats and vulnerabilities.

TELECOM/ ISP/ CARRIER

- Use tools that provide highly scalable network visibility for complete security monitoring and anomaly detection.
- Protection and mitigation of DDoS attacks.
- Comprehensive threat detection and mitigation, so that threats like Botnets, DDoS and Cryptojacking can been detected and blocked.
- Network performance monitoring and provisioning SLA.

INDUSTRIAL/ SCADA

- Use tools that provide highly scalable network visibility and separation of industrial control systems threats and traffic.
- Automate anomaly detection, identifying network security and operating issues before they cause damage.
- Fully understand industry regulations about risk, access and authorisation, and compliance.

MANAGED SERVICES PROVIDERS

- Create a centralised cyber security system, with role-based permission/ authentication for all networks, applications and devices.
- Invest in automation tools to perform security checks and enforce regulations.
- Use anayltics tools to perform intensive threat analysis and intuitive visualisations for results.