Practical implementation of Cybersecurity

Suresh Emmanuel

MBA, MSc Cyber security and Forensics, MBCS, CISM, CDPSE, CISA, CPISI, DISSCA, NCC-IDIC, ITIL V3.0, SIEM 101, ISO/IEC27001:2013 Lead Auditor, ISO/IEC 9001:2010 Lead Auditor

Chief Information Security Officer at Hatton National Bank PLC

Practical Challenges for Cyber security Implementation

- Prioritization;
- Budget – Cyber investments are expensive;
- Change resistance;
- Legacy systems;
- Lack of required skills;
- Leveraging of investment;
- Interoperability;
- Complexity;
- No quick or invisible ROI.

Approach to Practical Cyber security

- A governance framework for Cyber Security;
- Preventive Controls;
- Intelligence, monitoring, detection and analysis;
- Reporting, response and mitigation;
- Recovery.

Approach to Practical Cyber security

- A governance framework for Cyber Security;
  - Choose a framework that in line with high security standards
    - ISO/IEC 27001;
    - NIST Framework;
    - CIS Critical Controls;
    - PCIDSS, etc.
  - Implement and mature
  - Awareness and Culture
  - Sustainability and maintenance
    - KPIs/KRIs and measurements
    - PDCA

Approach to practical Cyber security

Protect

- Logical access and authentication protection
  - IAM;
  - PAM;
  - MFA.

- Network and communication security
  - NEXTGEN Firewalls;
  - Web Application Firewalls;
  - Advance Threat Protection;
  - SSL Inspection;
  - Risk based micro segmentation;
  - Deception.

Approach to Practical Cyber Security

- Protect
  - Data Security
    - Data governance;
    - Data classification and DLP;
    - DRM;
    - Data encryption on top of channel encryption.
  - Vulnerability management
    - Vulnerability discovery and remediation;
    - Supply chain security;
    - Virtual patching;
    - Legacy system care.

Approach to practical Cyber security

- Protect
  - Threat protection
    - Zero day exploits;
    - Zero day malware;
    - Exploit techniques prevention;
    - Cyber kill chain protection;
    - Minimal services, applications, ports, etc.
    - Whitelisting of services.

Approach to practical Cyber security

- Intelligence, monitoring, detection and analysis;
  - Threat Intelligence
    - Threats;
    - Techniques;
    - Potential campaigns, groups;
    - Internal correlation;
    - Prioritization.

  - Monitoring
    - 24*7 Security Operating Center;
    - Comprehensive asset onboarding;
    - Visibility and Correlation rules;
    - Predictive analysis.

Approach to practical Cyber security

- Detection and analysis;
  - Detection capabilities – Tools – SIEM, Visibility tools, etc.
  - Deception
  - Threat hunting
    - Reactive threat hunting
    - Proactive threat hunting
    - Indicators
    - IOCs - Compromises
    - IOCs – Concerns
    - IOAs – Attacks
    - TTPs – Tactics, Techniques and Procedures
      - ✓ Process pawning, Behavior, etc.

Approach to practical Cyber security

- Reporting and response
- Incident response and containment process
  - Who's doing what
  - Call trees
  - CERT support
  - Contractual agreements with Incident service providers
  - Supplier chain arrangements
  - Contain threat
  - Transfer threat
    - ✓ Cyber Insurance
  - Drill, Practice and fine tune

Thank you