Digital Transformation Solutions- Security Services

- **Security Assessments**
  - Network Penetration Test Assessment
    - Ingram Micro CEH certified resources
    - Identify vulnerabilities in your network defenses
    - Assume the role of a Hacker
    - Foot printing (Client Research), vulnerability scanning, attempted exploitation of identified Vulnerabilities, remediation recommendations in a final report.
    - Priced per External/Internal IP
  - Web Application Vulnerability Assessment
    - Ingram Micro CEH certified resources
    - Identify vulnerabilities in weak web application source code
    - Assume the role of Hacker
    - Foot printing, vulnerability scanning, attempted exploitation, remediation recommendations
  - Social Engineering Test Assessment
    - Ingram Micro CEH certified resources
    - Obtaining confidential information by manipulating and/or deceiving people through email and phone campaign to provide actionable data to educate employees and protect your company from Hackers.
  - **Vulnerability Scanning- vulnerability scanning, remediation recommendations.**
    - Ingram Micro CEH certified resources
    - Any Network Penetration Test will only test for known Vulnerabilities. Since the Security Landscape is constantly changing and Hackers are always coming up with new ways of gaining access, Ingram Micro recommends having the Network Penetration Test performed on an ongoing basis with monthly or quarterly Vulnerability scanning in between PEN Tests to detect for any new vulnerabilities.
    - Scan for known Vulnerabilities and provide a Final Report with Remediation Recommendations
    - No attempt to gain access to Vulnerabilities identified.
  - **Wireless LAN Penetration Test**
    - Ingram Micro CEH certified resources
    - Ingram Micro Will conduct a Wireless Controller and SSID review on Access Points, and SSID's which involves reviewing the configurations and verifying if Best Practices are being followed and if not what steps in order to remediate any issues.
    - Confirm AP Encryption method
    - Brute force attack
    - Scan for vulnerabilities if able to access network
    - Option to include Wireless Controller Configuration review

  - **Security Firewall Audit**
    - Ingram Micro CEH certified resources
    - Assess the risk of your perimeter defenses and provide recommendations and best practice on how to remediate vulnerabilities to harden defenses against today's modern attacks.
    - Best practice security audit report
    - Software vulnerability audit report
    - SysAdmin Audit Network Security (SANS) policy compliance report
    - Configuration report
  - Critical Security Controls Assessment Provide specific results vs. Best Practices for compliance with the Top Critical Security Controls.
    - Ingram Micro CEH certified resources
    - Authorized and Unauthorized devices and software.
    - Continuous Monitoring and Automation
    - Access Control for WiFi enabled devices
    - Penetration Testing
    - Secure configuration for servers, desktops and mobile devices
    - Application Software Security
    - Data Leakage Protection
  - Cisco ASA FirePOWER Network Threat Assessment
    - Ingram Micro CEH certified resources
    - Proof of value to show your clients the power of the Cisco ASA Next Gen Firewall with FirePOWER Service vs. their current firewall.
    - EndPoint Threat Assessment also available.
- NormShield (Ingram Micro exclusive Risk Scorecard)
  - Low Cost Rapid Cyber Risk Scorecard against 10 Risk Categories (60 Second Non-Intrusive)
    - 10 Risk Categories
      - Digital Footprint, Patch Management, DNS Security, Email Security, IP/Domain Reputation, Leaked Credentials, Fraudulent Domains, Web Security, Information Disclosure, Web Ranking
      - Sample Rapid Risk Scorecard
  - Comprehensive Cyber Risk Scorecard (Non-intrusive Scorecard on the market with >400 sources)
    - 20 Risk Categories
      - Digital Footprint, Patch Management, DNS Security, Email Security, IP/Domain Reputation, Leaked Credentials, Fraudulent Domains, Web Security, Information Disclosure, Web Ranking, Hactivist Shares, Social Network, App Security, SSL/TESL Sec, CDN Sec,

        Fradulent Apps, NW Security, DDOS Resilience, Brand Reputation, Attack Surface.
        - Sample Comprehensive Scorecard
  - SIEM Security Health Check
  - Enterprise Security Assessment
    - Gap Assessment (If no Compliance Requirement, recommend NIST Cyber Security Framework)
    - Internal + External Penetration Test
    - Social Engineering
    - Summary/Recommendations/Next Steps
  - SCADA Assessments
    - Supervisory control and data acquisition (**SCADA**) is a system of software and hardware elements that allows industrial organizations to: Control industrial processes locally or at remote locations. Monitor, gather, and process real-time data.
    - Organizations use SCADA systems to automate complex industrial processes, detect and correct problems, and measure trends over time.
    - SCADA systems are used in industries such as water management, building and facility management, traffic management, electric power generation, etc.
  - Onsite Security Penetration Testing
    - Access the building as an intruder
    - Gain access to sensitive/confidential data
    - Includes Physical Security Vulnerability Assessment
      - Identify weak Interior and Exterior physical security
      - Identify gaps in Video Surveillance
      - Identify data leakage concerns

- Cybersecurity Playbook- Solution book for our partners to gain access and insight to the Ingram Micro Security portfolio.

- **Managed Security Services**
  - 24x7 Security monitoring and alerting
  - Top-down view of your security operations through in-depth reporting and analysis
  - Monitoring and management of security infrastructure and systems.
  - Managed firewall, intrusion detection, vulnerability scanning, and endpoint management services.
  - Security operation centers providing 24/7 services designed to reduce the number of operational security resources and investments a Small to Mid-Market or enterprise needs to retain to maintain an acceptable security posture and adhere to compliance mandates.
  - Threat Intelligence
  - Security device management
  - Patch Management- An automated service for patching OS and third-party applications

- Initial Incident response
    - Compromise Assessment: Identification service for the discovery of potential compromise within the organization. Analysis of data collected during the engagement focuses on malicious activities performed within the organization, malicious outbound connections, and malicious applications
    - Incident Response Program Development- Assist in developing an internal incident response program that utilizes current capabilities, development of increased internal skills and knowledge, solutions gap and remediation plans, and roadmap for program maturation.
    - Incident Response Gap Assessment: Analyze the current people, processes, and technology of an organization as it pertains to each phase of the incident response life-cycle.
    - Incident Response Plan/Playbook Development: Assist in developing organizational Incident Response documentation based off of interviews of pertinent personnel, review of controls in-place, and our experience in delivering Incident Response services.
- UTM- Unified Threat Management (UTM) UTM appliances combine firewall, gateway anti-virus, and intrusion detection and prevention capabilities into a single platform. UTM are Firewalls that include security features such as IDS/IPS.
    - IDS/IPS- IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) both increase the security level of networks, monitoring traffic and inspecting and scanning packets for suspicious data. Detection in both systems is mainly based on signatures already detected and recognized.
- Managed SIEM (Security Information & Event Management)- **SIEM** is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. **SIEM** software collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. The software then identifies and categorizes incidents and events, as well as analyzes them.
    - Ingram Micro SOCaaS Vendors
        - ProVision by Foresite
        - ArcticWolf- Ingram Micro Market Development- Shawna Gentner
        - Binary Defense- Ingram Micro Market Development- IM Contact- Ali Casillo
        - Digital Hands- Inrgam contact- Jessica Cunningham
        - Alert Logic
    - Vendor SIEM Solutions
        - RSA Analytics
        - LogRhythm- Implementation & Management Services
        - IBM QRadar- Implementation & Management Services
- Advanced Threat Defense (ATD) Services

  - Supported Vendors are Fidelis and FireEye
    - Malware Identification
    - Zero-Day exploit detection
    - Malicious URL Blocking
    - Advanced Cyber Attack detection
    - Event Monitoring 24x7
    - Scheduled and on-demand reporting
    - Platform Maintenance and Updates
- EDR- Endpoint Management and Response Services
  - Supported Vendors are Cisco AMP for EndPoints and Carbon Black
    - Signature and behavior-based threat detection
    - Real-time event and state change monitoring
    - System Quarantines
    - Sandbox Integration
    - Attack chain visualization across the enterprise
    - Blocking of known threats through traditional A/V methods
    - Blocking of new threats through streaming prevention methods
    - Event monitoring 24x7
    - Maintenance and updates

- **Security Compliance & Framework Services (Governance Services)**
  - HIPAA- Health Insurance Portability and Accountability Act. Standards for the electronic exchange, privacy and security of health information
  - FERPA Assessment/Audits- The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Dept of Education.
  - FISMA Assessments/Audits- Federal Information Security Management Act of 2002- The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
  - PCI DDS/ QSA- (Qualified Security Assessor) Services- Payment Card Industry (PCI) Data Security Standard. Set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.
  - SOX- Sarbanes-Oxley- Protect investors from the possibility of fraudulent accounting activities by corporations.
  - GLBA- Gramm-Leach-Bliley Act- Federal law that requires financial institutions to explain how they share and protect their customers' private information.
  - GDPR- General Data Protection Regulation- Legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union.
    - Privacy Impact Assessment
    - Data Discovery and Access Controls

    - vDPO
- NIST- National Institute of Standards and Technology- Promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards. FISMA is the Federal Information Security Management Act of 2002, 44 U.S.C sec. 3541 et seq. FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347, Volume 116 Statutes, pages 2899 - 2970, H.R 2458). The bill requires that federal agencies provide information security, including those services provided by contractors or other sources. FISMA assigns responsibilities to National Institute of Standards & Technology (NIST) to provide standards and guidance to aid agencies in meeting the requirements of the law.
    - NIST CSF (Cybersecurity Framework)
    - NIST 800-171 – Specific guidelines to protect Confidential Unclassified Information (CUI), typically applied to Manufactures for Federal government and their subcontractors/vendors.
    - NIST 800-53- "Security and Privacy Controls for Federal Information Systems and Organizations" is a catalog of controls for information assurance. All Federal information systems must implement security controls listed in the catalog that apply for the FIPS 199 risk category system.
    - NIST 800-43- Systems Administration Guidance for Securing Windows 2000 Professional System
- DFARS- Defense Federal Acquisition Regulation Supplement. DoD-specific acquisition regulations that DoD government acquisition officials – and those contractors doing business with DoD – must follow in the procurement process for goods and services.
- ISO/IEC 27000- International Standards Organization- is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization’s information risk management processes.
    - ISO 27001- Specifies generic ISMS requirements suitable for organizations of any type, size or nature.
    - ISO 27002- Supporting documents to ISO 27001, giving guidance and advice on the implementation.
- COBIT- Control Objectives for Information and Related Technologies- is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance.
- HITRUST- Health Information Trust Alliance- A privately held company located in the United States that, in collaboration with healthcare, technology and information security leaders, has established a Common Security Framework (CSF) that can be used by all organizations that create, access, store or exchange sensitive and/or regulated data.
- SOC 2- The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to SOC 1/SSAE 18 which is focused on the financial reporting controls.

    - CJIS Criminal Justice Information Services– Standards for protection of data gathered and maintained by public services (police, fire, emergency) audited by FBI.
    - 23 NYCRR 500 - New York Codes Rules and Regulations - Requirements passed in NY State for financial sector. Insurers also may fall under NYCRR.
    - State requirements – Approximately 50% of US States have requirements for protecting data, and we can assess and consult on these requirements.
    - PIPEDA – Personal Information Protection and Electronic Documents ACT - is the Canadian federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of commercial activity.
    - FFIEC- Cybersecurity Assessment Tool to enable regulated financial institutions to assess their cybersecurity readiness. This tool may be used as a self-assessment. Regulators may also review the completed assessment during their examination.

- **Security Training Services**
    - Mile 2 Security Training Services
    - ERMProtect
    - Cybersafe Security Training
    - Vendor Certifcation Training

- **GRAD Program**
    - Prepare your sellers for the CyberSecurtiy market by giving them the knowledge needed to succeed. Ingram Micro Technical Enablement team developed content and training material designed as an intro to Cyber Security.

- **Security Practice Builder**- Work with Ingram Micro to build out a Security Practice for your company. Includes Self-Assessment based on NIST Standards, Scorecard, Discovery and Roadmapping with our Technology Consultants, Fill Security Gaps, Education & Training.
    - Goals of the Security Practice Builder include
        - Provide security-focused education and training to partners and their customers
        - Improve partners' security sales capabilities
        - Help partners expand their cyber and physical security portfolios
        - Assist with end-user cyber-security assessments and demand generation
        - Simplify the engagement process with Ingram Micro's security team

- **Security Services- Hardware & Licensing-** Ingram Micro Security Vendor Linecard… http://www.securitylinecard.info/
    - Preferred Security Service Provider Programs
        - ForcePoint- Web Security
        - Fortinet- next generation firewalls, antivirus programs, intrusion-prevention system, antispyware, antispam, VPN, wireless security, application control, web filtering

        - ZScaler- Global cloud-based information security company that provides Internet security, web security, next generation firewalls, sandboxing, SSL inspection, antivirus, vulnerability management and granular control of user activity in cloud computing, mobile and IoT environments.
        - Palo Alto- Next Gen/Advanced Firewall services
        - Symantec/BlueCoat- Cybersecurity Hardware, software & network management.
        - Sonicwall- Next-Generation Firewall; UTM; firewalls; VPN; wireless security; security appliance filtering spam, spyware, viruses and other malware
        - RSA- Network Security Software, Two-Factor Authentication, GRC, Anti-Fraud, Identity & Access Management
        - Pulse Secure- Network Access Control and IoT Security
        - Watchguard- Unified Threat Management (UTM) devices, next-generation firewalls, secure WiFi devices, cloud-based threat intelligence, device detection
        - F5 technologies- F5 focuses on the delivery, security, performance, and availability of web applications, as well as the availability of servers, cloud resources, data storage devices, and other networking components.
        - Cisco ASA

- **National Deployment Services**
    - Scale to larger projects
    - Scheduled installation services
    - Multi-Site- 100+ Sites
    - National Managed Workforce
    - Project Management and Access to Ingram Micro's Proprietary tracking toolsets to view project updates.

- **IT Asset Disposition (ITAD)-** Ingram Micro ITAD is the leading provider of secure, sustainable lifecycle service solutions for IT assets and consumer electronics worldwide. Ingram Micro IT Asset Disposition services reduce the risk, cost and complexity associated with securely managing & disposing of IT assets and consumer electronics throughout their lifecycle in compliance with environmental and data security regulations. With over 100 global locations, we manage the entire asset chain-of-custody seamlessly to provide secure and sustainable reverse logistics solutions.

- **Cloud Security Services**
    - AWS Security Configuration Reviews
    - Cloud Security Assessments

- **Application Security Services**
    - Mobile
    - Web

    - Secure Code Review
    - Application Security Training- For compliance

- **Security Audits and Consulting Services**
    - Consulting, gap/readiness assessments, and audits
    - Policy and Procedure Review.

- **Red Team Assessments-** A red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view. It is particularly effective in organizations with strong cultures and fixed ways of approaching problems.
    - Red Team assessments are performed to mimic actions of an actual attacker. MSSP (Managed Security Service Provider) performs activities as required from all security services to reach an end-goal (typically domain control or sensitive data access) as defined during the initiation of the engagement. Activities that may be performed to accomplish the service include Email Phishing, Phone Social Engineering, External and Internal Penetration Testing, External and Internal Application Penetration Testing, Physical Location Penetration Testing, and Wireless Penetration Testing.
    - Table Top engagement to simulate a Red Team engagement with Executives and all key parties

- **Blue Team Assessments-** A blue team is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation.

- **Death Master File security audits**- The Death Master File (DMF) is a computer database file made available by the United States Social Security Administration since 1980. It is known commercially as the Social Security Death Index (SSDI). The file contains information about persons who had Social Security numbers and whose deaths were reported to the Social Security Administration from 1962 to the present; or persons who died before 1962, but whose Social Security accounts were still active in 1962. As of 2009, the file contained information on over 83 million deaths. In 2011, some records were removed from the file.

- **Physical Security & Access Control Services**
    - Security Camera & Access Control Planning, Implementation & Support
        - Review & Design Services
        - National Deployments

- **IT Staffing Services**- Finding the right Security professional to fill a permanent or long-term project need can be frustrating and time consuming. Our experienced staffing specialists draw from our extensive database of skilled, proactively screened candidates to successfully place IT professionals in contract, contract-to-hire, and permanent positions. Ingram Micro IT Staffing Services leaves you free to drive sales and service customers by outsourcing the mundane tasks of recruiting and staffing technical professionals.

- Direct Hire Placement Services
- Contract Labor Services
- **CISOaaS & vCISO**- Chief Information Security Officer consulting/Staffing services. Sold as a block of hours or annual contract. Leverage the expertise of an experienced CISO.
    - Strategic information security roadmaps
    - Design and building of security related programs
    - Policy Development
    - Security Personnel/posture assessment
    - Regulatory compliance consulting
- Response Team options for getting hit with a Cyber Attack.
    - Team of technical resources to assist with reimaging and back up solutions.