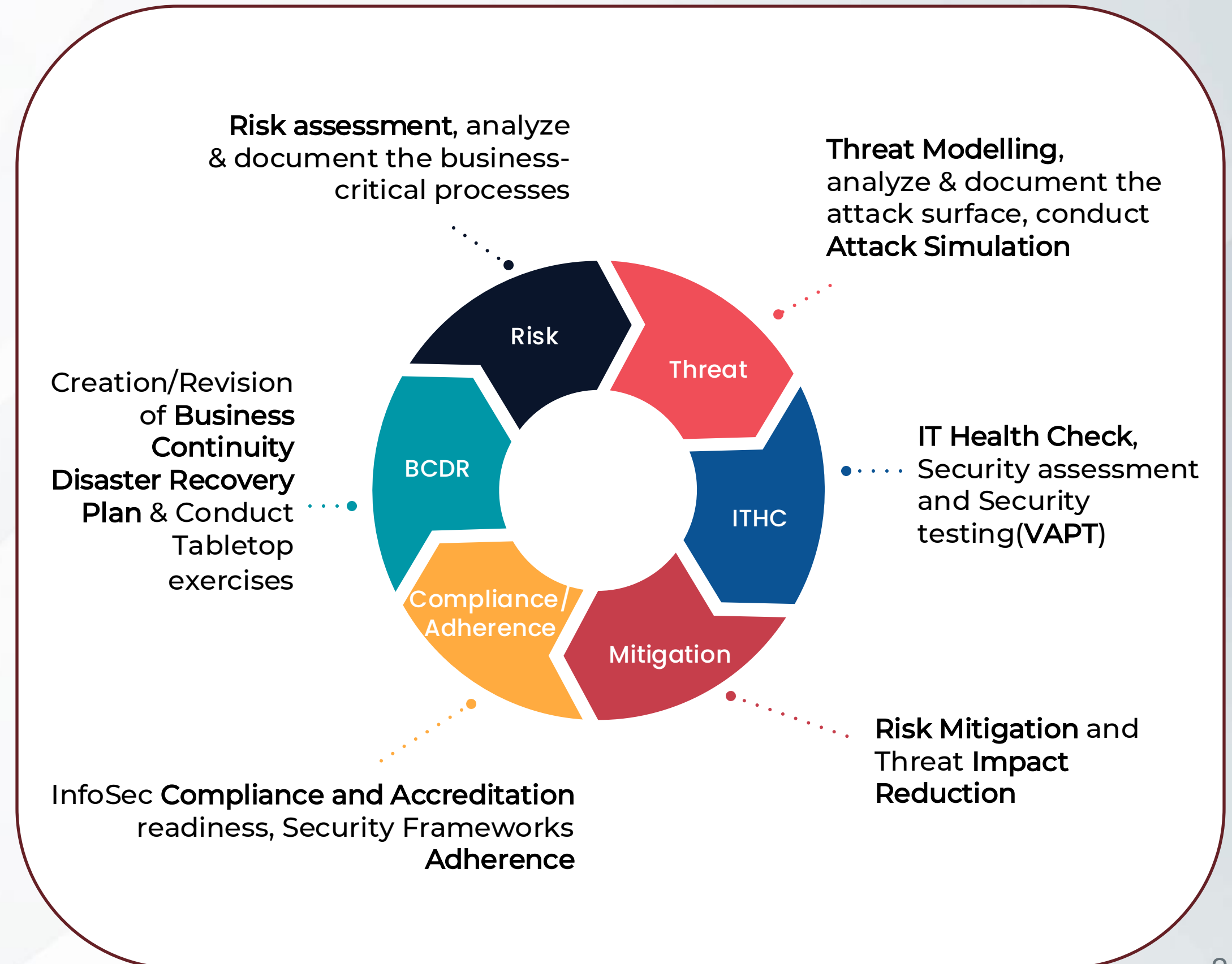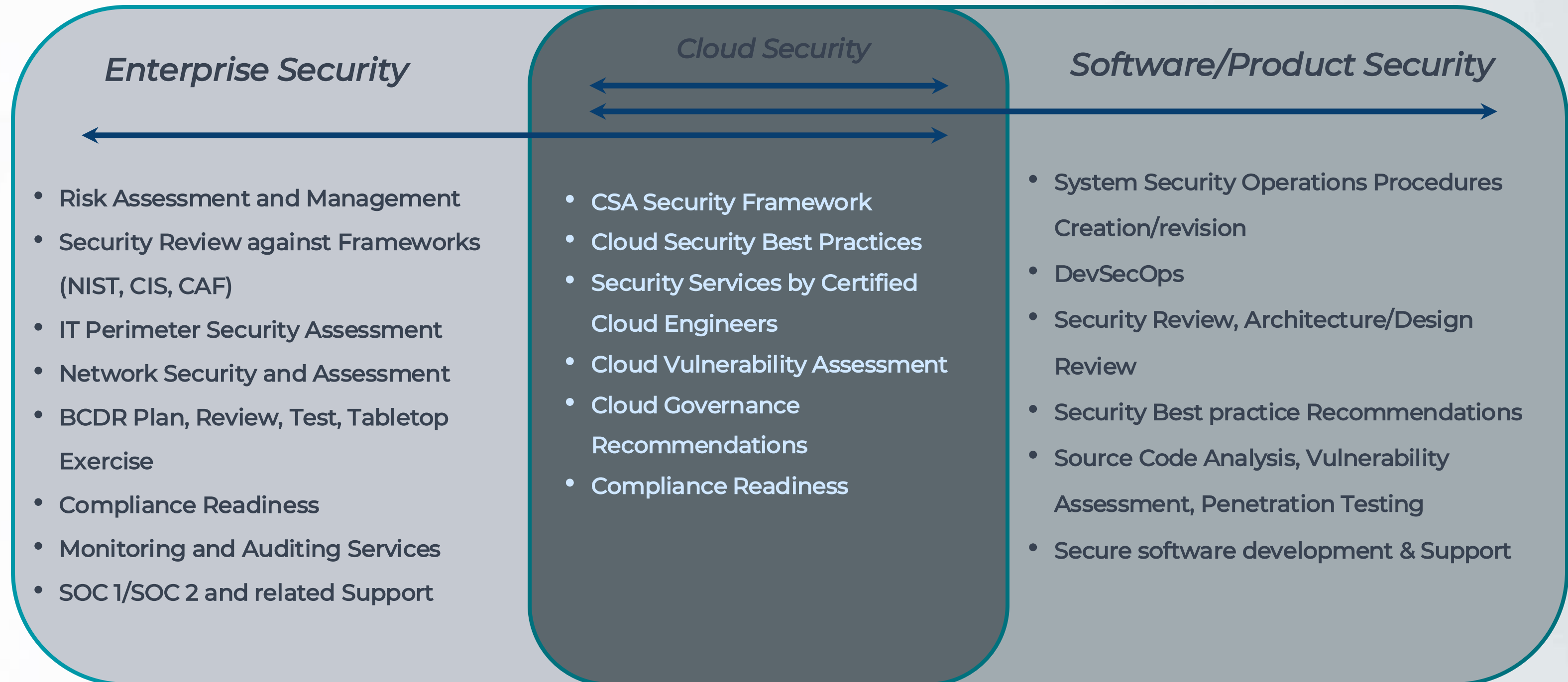# Digital Security Services

Accionlabs

Our Security Services and Framework

- Risk Assessment and Management
- Security Review/Assessment, Security Testing, Security Audit
- Security Review against Frameworks (NIST, CIS, CAF)
- Advisory/Resources to implement/address gap against Frameworks (NIST, CIS, CAF)
- IT Heath Check
  - Vulnerability Assessment and Management
  - Penetration Testing
- Compliance, Accreditation Readiness review, Gap Analysis and Gap mitigation
- Threat Analysis and Management
- Business Continuity Plan, Review and Management

Risk assessment, analyze & document the business-critical processes

Threat Modelling, analyze & document the attack surface, conduct **Attack Simulation**

Creation/Revision of **Business Continuity Disaster Recovery Plan** & Conduct Tabletop exercises

IT Health Check, Security assessment and Security testing(**VAPT**)

Risk Mitigation and Threat **Impact Reduction**

InfoSec **Compliance and Accreditation** readiness, Security Frameworks **Adherence**

Risk — Threat — ITHC — Mitigation — Compliance/Adherence — BCDR

Our Security Services Offerings

Enterprise Security

- Risk Assessment and Management
- Security Review against Frameworks (NIST, CIS, CAF)
- IT Perimeter Security Assessment
- Network Security and Assessment
- BCDR Plan, Review, Test, Tabletop Exercise
- Compliance Readiness
- Monitoring and Auditing Services
- SOC 1/SOC 2 and related Support

Cloud Security

- CSA Security Framework
- Cloud Security Best Practices
- Security Services by Certified Cloud Engineers
- Cloud Vulnerability Assessment
- Cloud Governance Recommendations
- Compliance Readiness

Software/Product Security

- System Security Operations Procedures Creation/revision
- DevSecOps
- Security Review, Architecture/Design Review
- Security Best practice Recommendations
- Source Code Analysis, Vulnerability Assessment, Penetration Testing
- Secure software development & Support

Engagement Models

Managed Security / Periodic Engagement

Ongoing Periodic, Quarterly or Annual engagement that will provide continual assessment and remediation cycles

Fixed Objective Engagement

One off, fixed engagement that focuses on a set of specific targets/objectives. As well as Resource/Staff Augmentation or SME pool provision

Project Based Engagement

Covers all information security elements of a project, starting with the initiation phase all the way culminating in a final ITHC before or at Go-Live

Our Competencies and Team Overview

Our Industry Certifications

- PCI DSS compliant
- HIPAA compliant
- CMMI v2.0 L3 certified
- ISO 9001:2015 certified
- ISO 27001:2013 certified
- ISO 27701:2019 certified

Our Security Team

- 30+ Core Consultants, 200+ Security Resources Across the Globe
- ISC^2 Certified professionals
- Certified Internal/external Auditors
- Certified Ethical Hackers
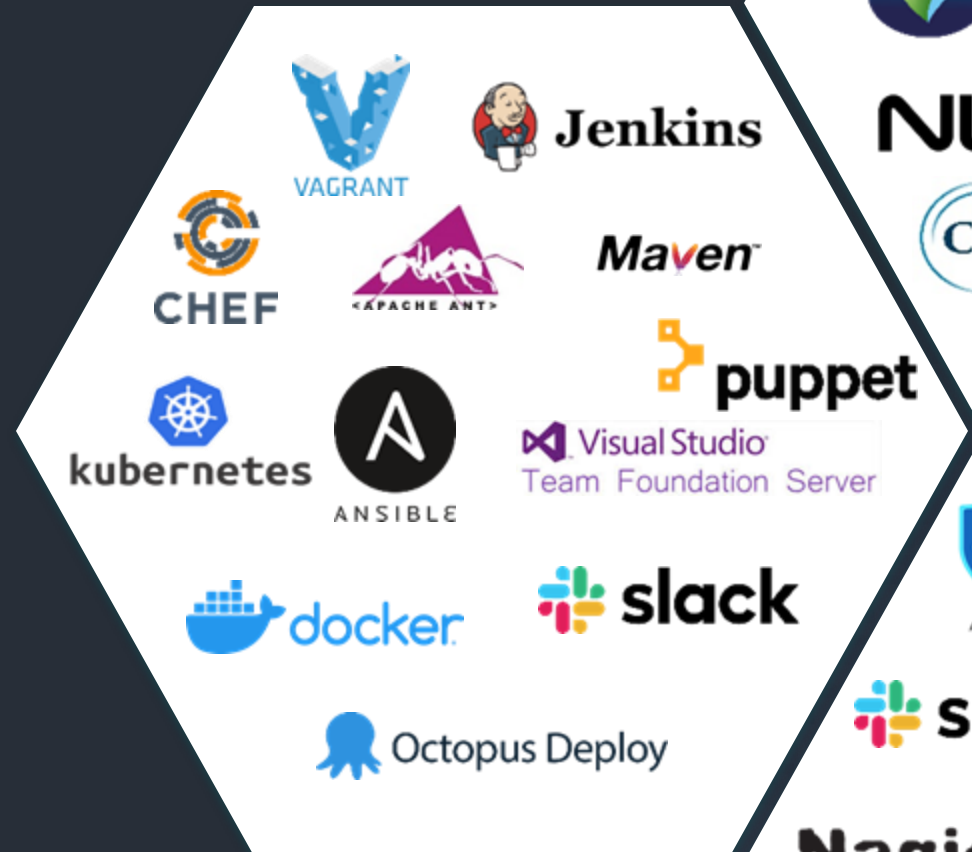- Certified DevSecOps

Our Security Toolkit
Non-exhaustive list

Security Standards, Frameworks & Accreditations

HIPAA · FISMA · OWASP · PCI-DSS COMPLIANCE · CSA cloud security alliance · ISO 27001 · CYBER ESSENTIALS · MITRE ATT&CK · NIST · HITRUST · HL7 FHIR · CIS Center for Internet Security · CAF by National Cyber Security Centre · SOX Sarbanes-Oxley Compliance

Security focused DevOps Tools

VAGRANT · Jenkins · CHEF · APACHE ANT · Maven · kubernetes · ANSIBLE · puppet · Visual Studio Team Foundation Server · docker · slack · Octopus Deploy

Security Testing Toolset

BURPSUITE · OWASP Zed Attack Proxy · threat stack · cloudMAP · VERACODE · BLACKDUCK · HACKER GUARDIAN · metasploit · KALI · sonarqube · Nessus vulnerability scanner · OpenVAS Open Vulnerability Assessment Scanner · WIRESHARK

Security Monitoring

Azure Defender · Azure Sentinel · AWS Security Hub · slack · sensu · WhatsUp Gold Progress · Nagios · solarwinds · wazuh · Prometheus · OpenNMS · splunk> · PRTG NETWORK MONITOR · Qualys · elastic · servicenow · ZABBIX

© 2024 Accion Labs

Our Controls and Practices

- Information Security Management System with over 150 Security controls from ISO, PCI-DSS, HIPAA
- Robust Security Awareness Training Program and Assessments
- Periodic reviewing Risk Assessment Plan, Risk Mitigation Plan and Business Continuity Plan
- Protection of client and client's information
  - Designated Secure PCI-DSS Section with Physical Security Controls
  - Site to Site VPN, Strong Firewalls with modern Rulesets
  - Virtual Desktops, IP Whitelisting
  - Benchmarked OS images, centralized Security Updates, Remote Wiping where necessary
- Annual Business Continuity and Disaster Recovery Exercise
- Quarterly internal audits and annual third-party audits
- Quarterly Vulnerability Assessments and Penetration Tests
- Continues self monitoring and maintaining Security Posture enables us to achieve and maintain Excellent Security rating
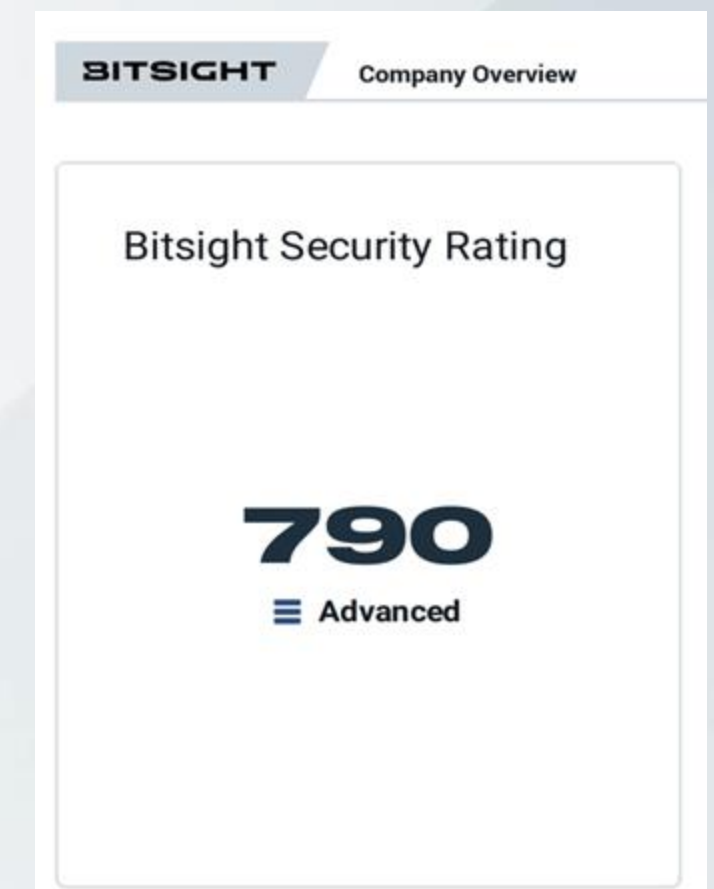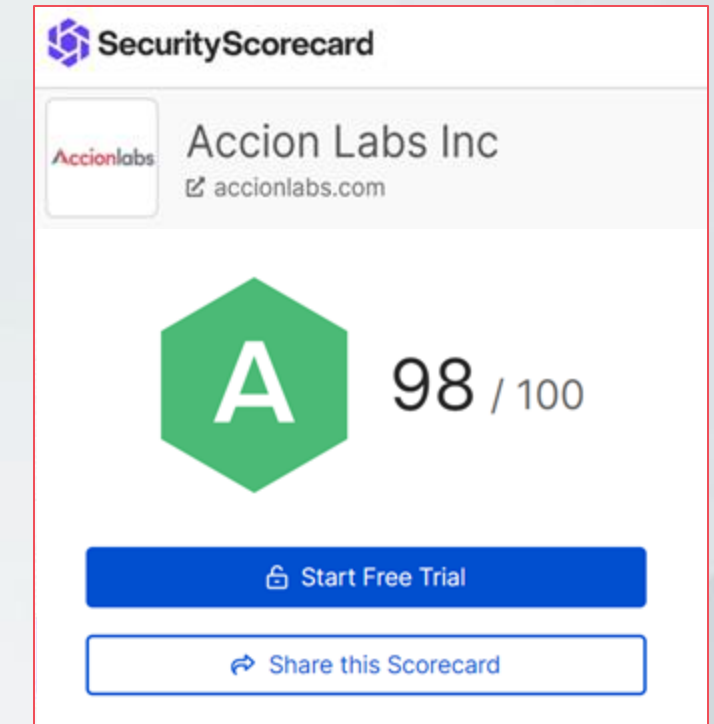
Success Stories

EDC model for an Application Security Giant - VERACODE

Security Challenge/Objective

- VERACODS's legacy Dynamic Analysis App test platform (DAST) had monolithic architecture without optimized value delivery & observability implementation.
- Customer was not able to scale the software teams thus slow down delivery cycles.

Solution

- Utilisation of our Program Security with EDC approach
- With integrated partnership, Accion's engineering and cloud native teams were put in place in short amount of time.
- Key part of the solution worked by teams included:
  - optimal use of cloud capabilities (use of managed EKS, KMS)
  - microservices architecture & development process optimization.
  - monitoring/observability platform (Datadog) implementation

Business Impact

- As a result, shorter time to market for the product features via rapid scaling and faster delivery.
- Reduced operational/maintenance cost of the platform technology by leveraging industry standard toolset.
- Reduced risk by simplified processes

Security Compliance for a Mental Health provider - MindWeal

Security Challenge/Objective

- Build a HIPAA Compliant Platform for a North American mental health provider with required Security Controls.
- Security Objective – Provide Appropriate organizational, administrative, physical & technical safeguards and procedures to be implemented to protect the security of ePHI, to prevent unauthorized or accidental access, damage, loss or other risks presented by data processing
- Provide and Maintain Security & Quality Process documentation

Solution

- Utilising our Software Security offering
- Designed Security Architecture in Accordance with HIPAA Security Requirements
- Defined Cryptography Standards for handling & transporting PII and ePHI.
- Conducted SAST/DAST & HIPAA assessment of the platform for HIPAA Audit Attestation.
- Analyzed and confirmed PCI DSS compliance in handling Credit Card data flow.
- Configured appropriate monitoring systems to identify and alert threat on the platform.

Business Impact

- Platform achieved HIPAA compliance with a very few low numbered observations
- Advantage over similar competitor businesses
- Client's business plan progressed without deviation
- With this HIPAA compliance for the MindWeal as Organization has a strong foundation

Security Advisory – World Health Organisation

Security Challenge/Objective

- Secure the data Processing for a United Nations agency that connects nations, partners and people to promote health so everyone, everywhere can attain the highest level of health
- Security Objective - Appropriate organizational, administrative, physical & technical safeguards and procedures to be implemented to protect the security of personal data, to prevent unauthorized or accidental access, damage, loss or other risks presented by data processing

Solution

- Utilisation of our Program Security and Cloud Security offering
- Dedicated Security SME
- Security Review of Cloud Architecture
- Conduct Risk Assessment and Outline Risk Management Strategy
- Prioritizing mitigation strategies based on risk of the Vulnerabilities.
- Update CI/CD pipelines with enhanced Security Controls
- Update DevOps pipelines to add Security Tools

Business Impact

- Five folds increase in compliance with WHO Information Management and Technology (IMT) policies and guidelines
- Lowered the risk of a security breach
- Increased communication integrity
- Significantly reduced attack surface
- Reduced the exposure to the public networks

Security Posture Management – a British Fintech

Security Challenge/Objective

- A health insurance platform's Security assessed to provide the status of the Web application's Security Posture
- Security Posture Management via Complete Vulnerability Assessment.

Solution

- Utilising our Software Security offering
- Security Architectural review
- Attack surface analysis and Threat modelling
- Vulnerability Assessment with Penetration testing based on the Prepared threat models
- Conducted Regulatory Compliance readiness review

Business Impact

- Improved the stack holder's confidence in the product
- Laid the foundation for future regulatory and compliance audits
- Provided much needed time and resources bandwidth before go live for the client.
- Reduced the risk of a security breach and the associated costs and damages

Assura+Protect

Security Posture Management - IAEA

Security Challenge/Objective

- Provide Security Assurance to IAEA for a digital platform that is an Regulatory Inventory Management and Audit System for machines that uses radioactive material
- Analyze Security Posture followed by Security Enhancements and Improvement in Security Posture

Solution

- Utilising our Software Security offering
- Architectural review
- Provided assistance to improve security design
- Implemented Cryptographic controls
- Attack surface analysis and Threat modelling
- Vulnerability Assessment with Penetration testing based on the Prepared threat models
- Provide mitigation Strategy for the observed vulnerabilities

Business Impact

- Improved Security Posture
- Increased confidence of the IAEA participating countries
- Timely release of the Inventory Management and Audit Platform

IAEA
International Atomic Energy Agency

Security Testing - UNICEF

Security Challenge/Objective

- Complete Security Assessment for Various Web Applications for UNICEF:
  - Country Portal
  - Supply Chain management
  - Malaria Toolkit
  - Health Account Production Tools
  - Covid-19 Dashboard
- Improve Security Posture

Solution

- Utilising our Software Security offering
- Architectural Security review
- Attack surface analysis and Threat modelling
- Vulnerability Assessment with Penetration testing based on the Prepared threat models

Business Impact

- Improved Security Posture
- Increased confidence of the IAEA participating countries
- Timely release of the Inventory Management and Audit Platform
- Reduced the risk of a security breaches and the associated costs and damages

Industry Segments

Talent at Accion

Talent presence

Americas
600+

Europe
110+

Asia
4290+

Gender Diversity

Male : Female
72 **28**

Number of Nationalities

20+

Learning in CY24

Instructor led Total person learning hours:
44891.48

Udemy Total person learning hours:
63193.27

Voluntary attrition is around
20%

Amber, our Chief Listening Officer

Accion Labs India – **Great Places to Work certified**

Employee Engagement Score
8 2

%age of Accionites who have given positive mood score
88.11%

89% of Accionites say this is a great place to work!

Focused ESG initiatives that help us do the business **"right way"** making our business purposeful, ensuring long term successes and wins

Partnerships and Alliances

Thank You

For more info please visit www.accionlabs.com