Case Study

UNDER DEFENSE

Virtual CISO for FinTech

Client Pains

Setting up security processes with limited IT and security resources

Receiving and filling out lots of security questionnaires from prospects

Meeting compliance with SOC2 Type I & II, HIPAA compliance, GDPR, CCPA, NY SHIELD Act

Possibility of being hacked and client data compromised that leads to competitors displacing your start-up

Checking the application security flaws when getting displayed at SalesForce platform

Adapting business to future challenges and aligning technical & business goals with security standards

UNDER DEFENSE

Business goals reached

Compliance

Set-up security processes

Introduce and follow security RoadMap

Automatization

- Achieved SOC 2 type II and GDPR readiness
- Minimized the Cost of the Security Issues Resolution
- Reduced operating costs using Splunk
- Continuous educational trainings and assessment helped to strengthen the security posture of the organization

UNDER DEFENSE

Remote Security Advisor activities

1. Take care about Information security leadership
2. Security Point-of-Contact for All Issues
3. Building security Strategy & Roadmap
4. High level cost estimates for budgetary purposes
5. Project planning and execution
6. Testing implemented policies and procedures
7. Guidelines & Best Practices
8. Communication with Top management on business risks and threat scenarios

UNDER DEFENSE

Solution/Service Title	Virtual CISO for FinTech Startup
Client Overview	SaaS-based accounts receivable management platform which includes: real-time accounts analytics, reporting and collecting data. It's a single point of record for each invoice with notes, disputes, emails, calls and contacts with CRM functionality.
Client Challenge	Working within Financial Industry our client must comply with the following regulations: SOC2 Type I & II, HIPAA compliance, GDPR, CCPA, NY SHIELD Act
Technologies	Amazon Web Services, Splunk Enterprise, Wazuh, ESET Endpoint Protection, Cisco Meraki System Manager
Key Benefits	Our client has received a dedicated person that sets up, maintains and continuously enhances cyber-security controls and processes in the company.
Results	After we defined and resolved all critical areas our client successfully passed SOC 2 Type I, Type II and HIPAA/HITECH audits. Also, our vCISO has implemented Secure Software Development Life Cycle (SDLC) model including establishing Incident Response, Disaster Recovery, Business Continuity processes

UNDER DEFENSE

vCISO project stages

1 Security Assessment

Indicating weak points at the security posture and producing strategic recommendation to close these gaps

2 Secure SDLC

Minimizing the cost of the security issues resolution and implemented best security practices of Incident Response, Disaster Recovery, Business Continuity processes

3 Security Operations

Implementing best security practices with AWS infrastructure optimization, security monitoring with Splunk SIEM tool and preparation to SOC1, SOC2

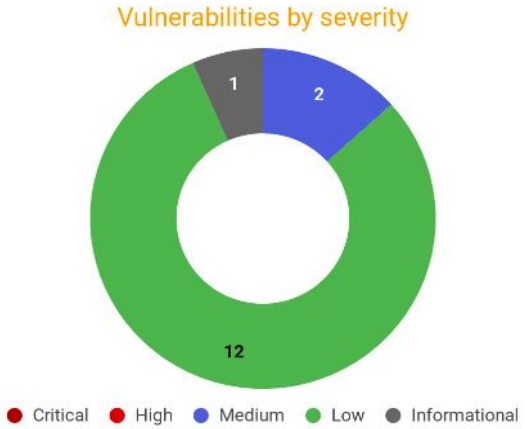
4 Security Trainings

Continuous employee education by conducting a series of trainings in Cybersecurity Awareness and testing their readiness with social engineering

UNDER DEFENSE

Penetration testing

- Application Penetration Testing
- Infrastructure Penetration Testing
- Organization Penetration Testing
- Remediation recommendations
- Remediation testing



Security experts performed manual security testing according to OWASP Web Application Testing Methodology, which demonstrate the following results.

Severity	Critical	High	Medium	Low	Informational
# of issues	0	0	2	12	1

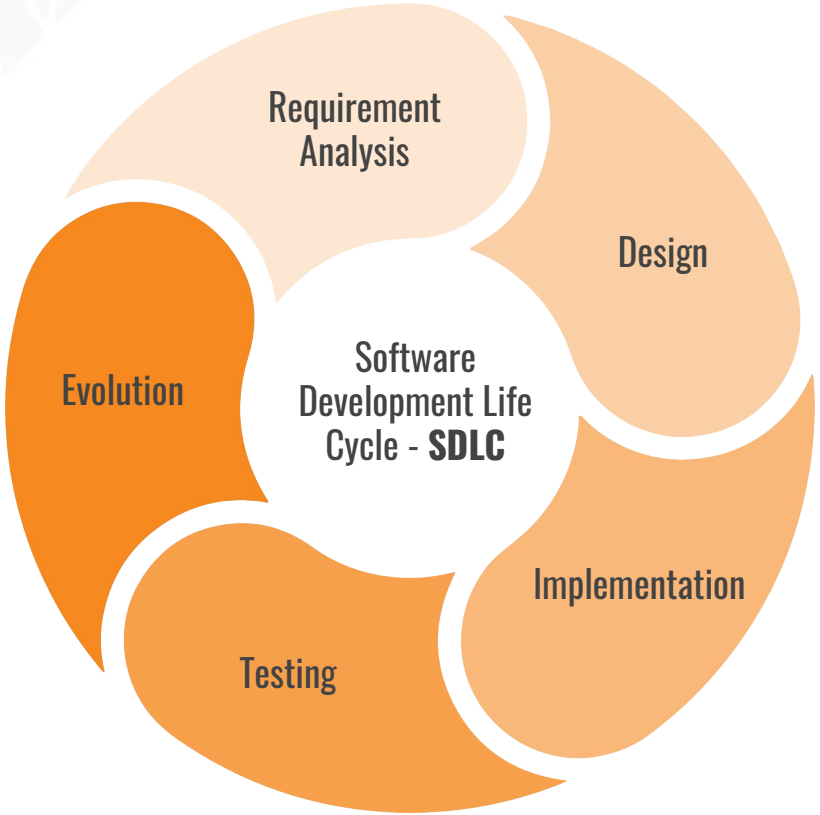
Severity scoring:

- Critical - Immediate threat to key business processes.
- High – Direct threat to key business processes.
- Medium – Indirect threat to key business processes or partial threat to business processes.
- Low – No direct threat exists. Vulnerability may be exploited using other vulnerabilities.
- Informational – This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

UNDER DEFENSE

Secure SDLC

- Secure Development Trainings
- Application and Organization Thread Modeling
- Non-Functional Security Requirements
- Supply Chain Security
- Static and Dynamic Code Analysis
- Source Code Leak Protection
- Penetration Testing



UNDER DEFENSE

Setting up compliance

We helped our client build Security Roadmap and follow the mapped steps to achieve readiness with compliance audit and match the specified regulations:

- SOC 2 Type I
- SOC 2 Type II
- HIPAA/HITECH
- ISO 27001
- PCI DSS
- CCPA
- NY Shield Act
- UK DPA
- GDPR

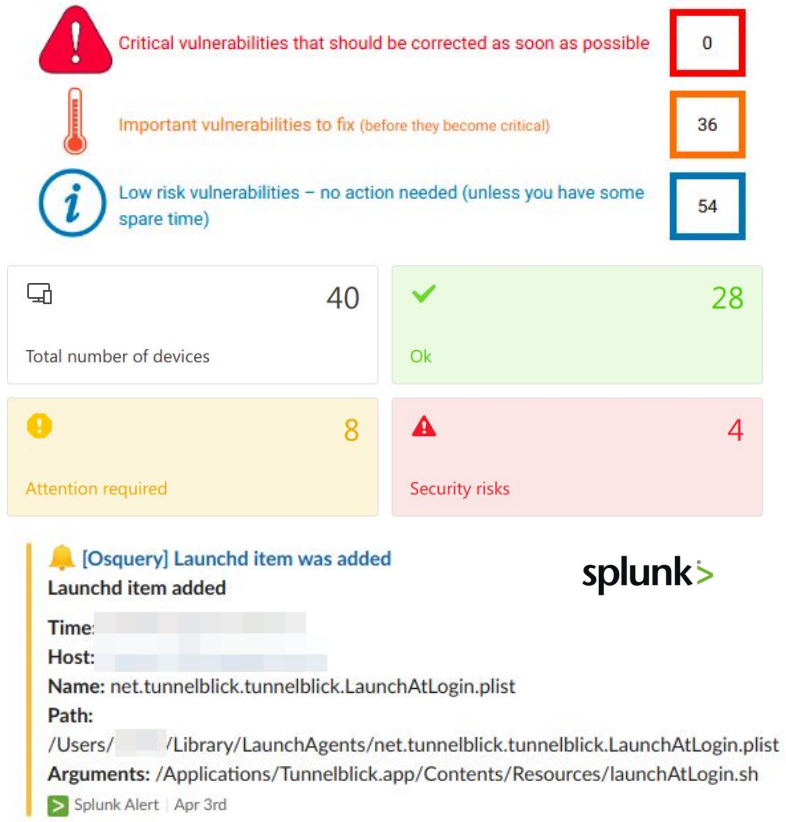
The assessment was conducted in two phases:

1. Setting up required technical controls
2. Setting up required organizational controls (Policies and Procedures)

UNDER DEFENSE

Security Operations

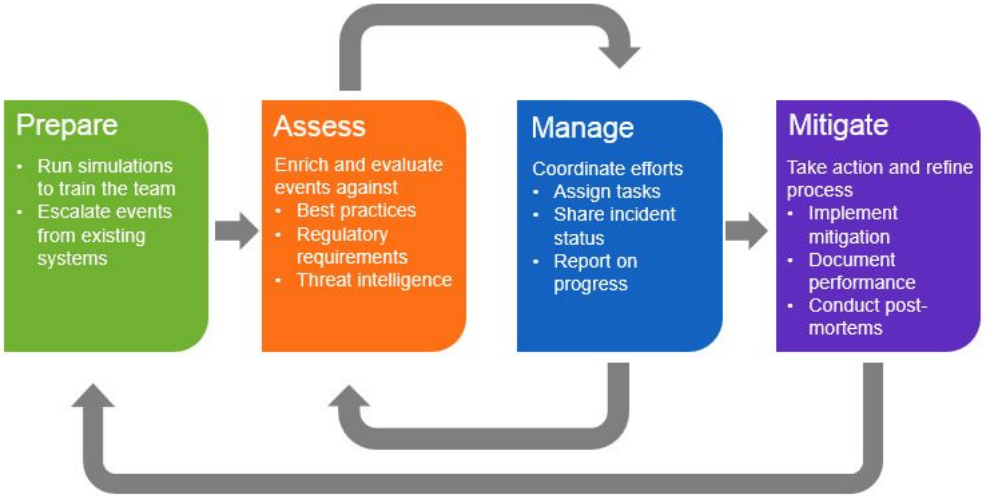
- Asset Management
- Vulnerability Management
- Endpoint Management & Protection
- Network-based Intrusion Detection and Prevention
- Host-based Intrusion Detection and Prevention
- Cloud and Container Security



UNDER DEFENSE

Incident Response

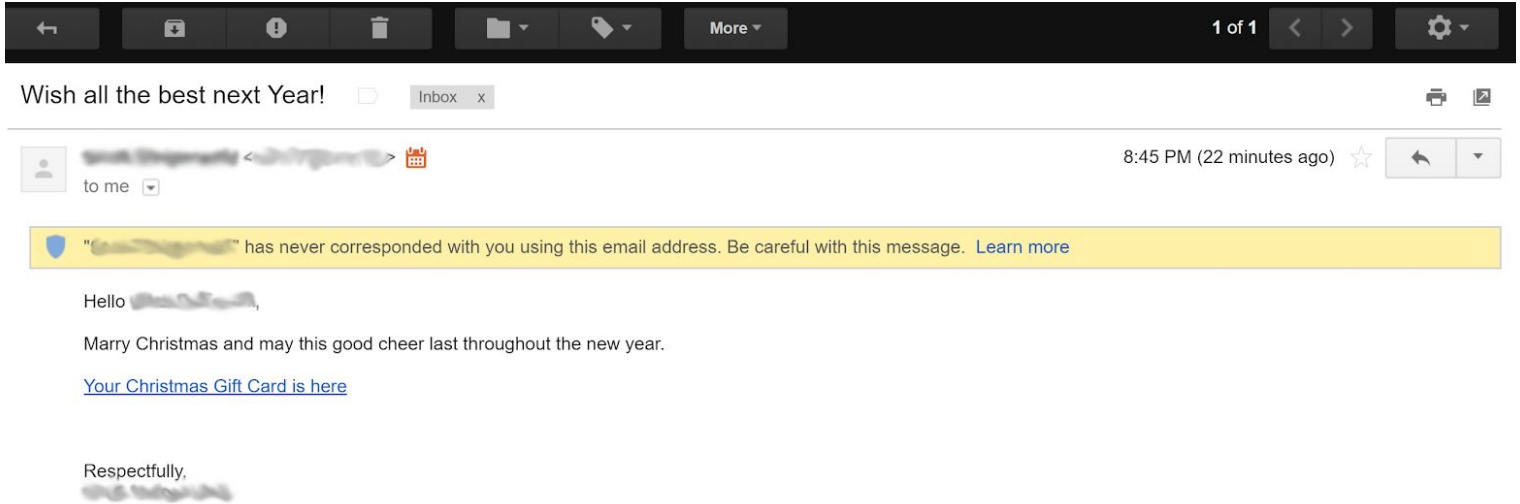
- In-house Incident Response process development
- Incident Response automation
- Incident Response testing and tabletop exercises
- Communication with law enforcements and data protection authorities



UNDER DEFENSE

Incident Response to a suspicious email attack

We have investigated the file attached in our Malware Lab environment and detected malware for Windows users. vCISO reviewed the database and detected all recipients of this email and blocked the addressant user.



Security Education Program

- Onboarding Security Awareness
- Awareness Trainings Annually
- Secure Development Trainings Annually
- Social Engineering Testing

UNDER DEFENSE

Thank you for your trust

Call us now at +1 929 999 5101