Strategy Document for Product Security V1.0

Presented by Product Security Team

Author: Vartul Goyal

CONTENTS OF DOCUMENT

Introduction about Security Strategy

Business companies create and uphold strategic plans for the majority of the tasks they perform. Strategic plans outline the necessity of a given action, its impact, and the underlying reasons that motivated it. Any organization's security plan must begin with a thorough examination of its operations. Therefore, a security strategy is a crucial document that outlines the processes required for a business to recognise, address, and manage risks while remaining compliant. A comprehensive and dynamic security strategy with the flexibility to react to any kind of security attack is effective. The process of creating a security strategy is complex and includes an initial assessment, planning, execution, and ongoing monitoring. A mix of policies, processes, access management measures, communications systems, technologies, and systems integration techniques may also be used to address all potential risks and vulnerabilities.

Information assurance and security efforts that the organization must launch to improve the protection of information and related technologies are defined and prioritized in the security strategy document. When possible, an organization should combine previously identified and completed projects, define each endeavor, describe the basic risks it addresses, and lay the groundwork for future refinement by senior management.

Additionally, the security strategy planning process has to identify any important dependencies associated with the initiative in order to facilitate higher-level review of initiatives that can be implemented when necessary. Plans are broken down into categories based on the number of months, quarters, half-years, and years.

Building Blocks of an Effective Security Strategy

A security strategy is the organization's plan for lowering cyber risk and safeguarding its assets from potential threats online. Plans for cybersecurity are frequently made with a three to five-year horizon, but they should be updated and reevaluated frequently.

A good security strategy may evolve over time. It is a living, breathing document. It must adjust to the current threat landscape, put tools and best practices in place, and take other steps to protect the firm from threats both internal and external.

1. Risk Inventory

A thorough inventory of all digital assets, staff, and vendors is the first component of a successful cyber security strategy. Organization and discipline are essential. It is simple to assess internal and external threats and weaknesses with a current inventory of assets. Additionally, it assists in identifying long-forgotten or unattended IT infrastructure problems.

Start by mapping data, assets, and threat landscape.

Classify your Data

- Public data – Any data share with the public—for example, website content.
- Confidential data – Any confidential data that may be shared with 3rd parties or external legal entities. Access to this data should require a Non-Disclosure Agreement (NDA).
- Internal use only data – Similar to confidential data, but should only be shared internally.
- Intellectual property data – Critical core business data that would damage the company's competitiveness in case of a breach.
- Compliance restricted data – Storage of restricted compliance data such as CMMC, HIPAA, HITRUST, NIST must comply with the mandated security framework.

Map Your Assets

- Software – Maintain a container for authorized software.
- Systems – Use a Central Management Database (CMDB) to map assets back to a system or asset owner.
- Users – Use a directory to catalog and assign users into groups and roles. Keep it up to date.
- Identity – Track user assignments to assets based on their current position or function.

Know Your Stack

- Assets + Vendors – Monitor contractors or 3rd party vendors with access.
- Infrastructure – Identify all network exit and entry points offline and online.
- Connected environments – Ensure network layouts are available and up to date. If users use cloud infrastructure environments, ensure infrastructure diagrams are available too.

2. Communication & Collaboration
If user want an effective cyber security strategy, we need everyone to be on the same page. Therefore, consistent communication with every employee, manager, and vendor is a must.

3. Cybersecurity Framework
To ensure the user is not missing anything and to comply with industry standards, it's better to start building a cyber security strategy with the help of a proven cyber security framework. These frameworks are blueprints of policies, goals, and guidelines that explain all cybersecurity activities within an organization.

NIST CSF – The NIST cybersecurity framework is based on the best practices and guidelines for identifying, detecting, and responding to cyberattacks. It outlines specific actions an organization can take to get users started with the security strategy.

ISO/IEC 27001 -The ISO/IEC 27001 is a certificate created by the International Organization for Standardization. The ISO/IEC 27001 framework achieved international standards for validating a cybersecurity program — internally and externally.

ISF – The standard of good practice was issued by the Information Security Forum. This framework is a business-focused, practical guide that helps identify and manage IT risks in organizations and supply chains.

4. Security Policies
To realize cybersecurity strategy, user will need to create and enforce security policies. Security policies serve as the company-wide rulebook of cyber security strategy.

When developing cyber security policy, consider the following:

- Password requirements

- Zero-trust and minimal access permissions
- IAM & credential management
- Protecting sensitive data
- A cyber security incident response plan
- Monitoring and identification any unusual activities

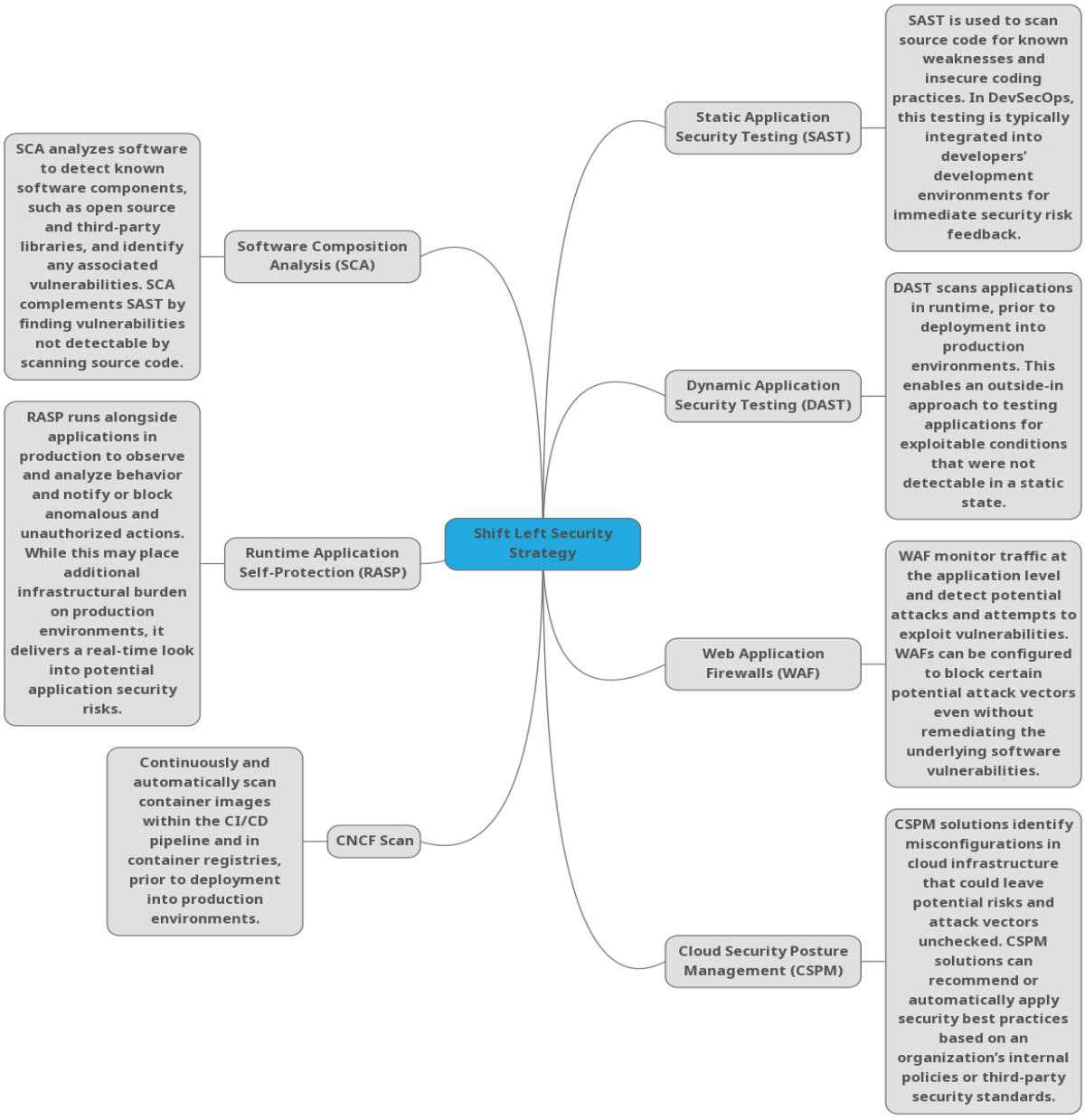
5. Tech Stack & Automation
Having a cyber security plan and policies is excellent, but how can users protect what they can't see? Especially in software development lifecycle? The best thing users can do for a company's cyber security efforts is automating the threat detection process, especially when it comes to code security threats.

6. Multiple Lines Of Defense
If the user is serious about security strategy, ensure it includes multiple lines of defense. Threats to code and data can come from internal and external sources. So don't just pick one or two defense tactics or tools, but rather layer access control with monitoring and automated scanning.

7. Zero Trust & Access Control
Abusing access privileges is one way for attackers to penetrate the corporate work environment after finding a vulnerable entry point. This threat is ubiquitous since the increase in remote work in the past three years.

Security Strategy using Shift Left Security

Below are the parameters discussed about core technical security deliverables during security strategy(specially in case of Shift Left Security Model) required by every year. Half of the organization is not dependent on this model and it can save a lot of cost for the organization.



Vulnerability Management

- **Continuous Vulnerability Identification & Discovery** - continuous vulnerability scanning via different vulnerability scanners
- **Vulnerability Triage** - calculating severities/risk

- **Vulnerability Reporting** - attributing vulnerability tickets to the right owner
- **Vulnerability Remediation** - setting SLAs and enforcing them
- **Centralized Vulnerability Tracking** - track vulnerabilities reported from various scanners in one place

Security Partnerships

- **Secure SDLC (Secure Software Development Life Cycle)**
    - RRA (Rapid Risk Assessment)
    - Tech / Architecture Design Reviews
    - Threat Modeling (App + Deployment)
    - Secure Code Review
- **ASVS** (Application Security Verification Standard)
- **Security Scorecards**
    - Dashboard to get data from various tools and bubble up that data into a score → show this score in Github repos (as badges) and gamify with instructions on how to improve the score
- **Security Champions**
- Customized **Security Training & Education**

Security Tooling & Operations

- **KPIs / Metrics** - things user want to report on to the C-suite to show progress
- **Security Scanning Tools**
    - Setting up SAST, DAST, SCA, etc.
    - Maintaining and fine-tuning the tools
    - CI/CD Integration
- **Secure Defaults** - secure by default libraries & design patterns
    - Example - Some secure default policies could be set at Github org level using AllStar
- **Bug Bounty**
- **External Pentests**
- **Product Security Incident Response** - setting up Product Security IR processes and runbooks
- **Automated Application Security Platform** - think of this like a one-stop security dashboard that has data about all things security constantly getting updated

Security Strategy Planning on Yearly Basis

Below are the few parameters to decide about execution of **Security Planning on Yearly Basis** at a high level

WorkStreams	Security First Year	Security Second Year	Security Third Year
Vulnerability Management	Vulnerability Triage	Continuous Vulnerability Identifications and Discovery	
	Vulnerability Reporting	Centralized Vulnerability Tracking	
	Vulnerability Remediations - Manual Follow Ups	Vulnerability Remediations - Automated SLA Enforcement	
Security Partnerships	Establish Security SDLC Processes	Automated Secure SDLC	Customized Security Training and Education
		ASVS	
		Security ScoreCards	
		Security Champions	
Security Tooling & Operations	Manual KPI/Metrics	Automated KPI/Metrics	Bug Bounty
	Security Scanning - SAST	Security Scanning - SCA	Security Scanning - Secrets
	Security Scanning - CI/CD Integration	External Pentests	Automated AppSec Platform
	Security Scanning - Tool Maintenance & Tuning		Product Security Incident Response
	Security Scanning - DAST		
	Secure Defaults		

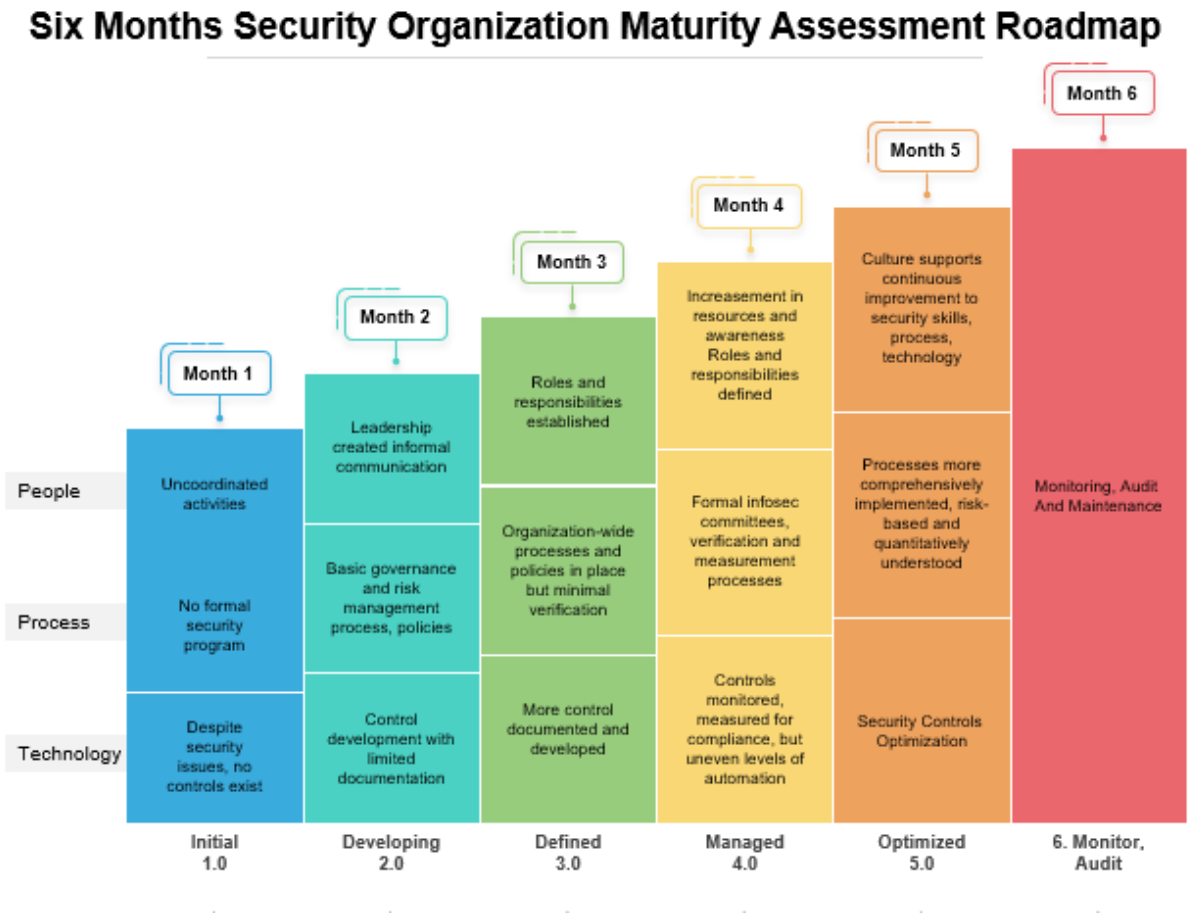
Security Strategy Controls

When defining the security strategy for any product based organizations, we have to consider below **Security Strategy Controls**

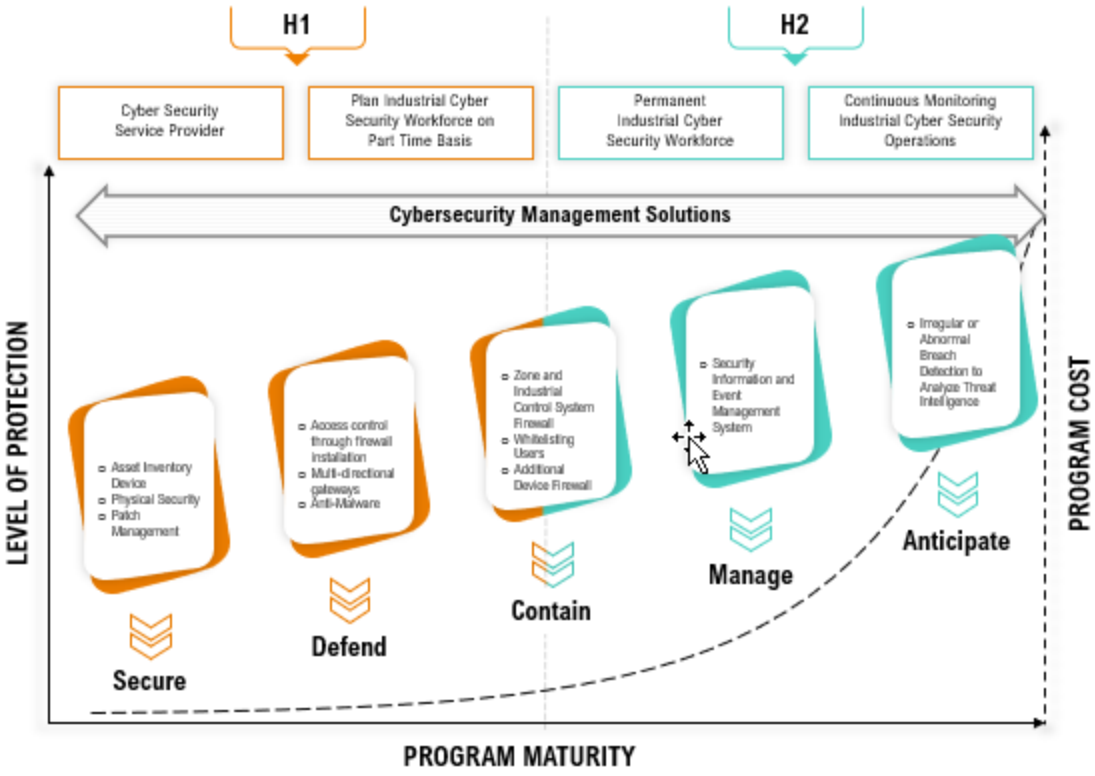
Security Strategy Controls	Security Strategy Dependent Parameters
Password security	Passwords Stored Hashed and Salted
	Enforceable Minimum Password Strength Options for Administrators
	Enforceable Password Expiration Options for Administrators
	Password Reuse Prevention
	Password Reset Controls
	Multifactor and 2-Factor Authentication Enforcement Option for Administrators
Security Activity Notifications	There are several incorrect login attempts when a user enters an incorrect password, yet with a correct email address or username.
	There is a login from a new device or browser.
	Logging in from a different geographic location than usual.
Password Attempt Threshold/ Account Lockout	More than 5 failed login attempts within 6 hours from 1 user
	More than 50 failed login attempts from 1 IP address within 1 hour
Admin Security Controls	Give administrators the tools and features to effectively administer the accounts in the application
Subject Access Request	Data protection and data privacy regulations that are popping up across the globe mean having the tools to respond.
Third-party Data Backup Support/Data export Support	
Single Sign-On Support	
Soft Delete	When users flag items or select items to delete, a good application feature to have is a soft delete feature. A soft delete application feature means that a deleted object is not actually deleted, at least initially.

IP Whitelisting	
Active Directory/Google, etc Employee Directory Features	More commonly today there are cloud-based IAM solutions being offered such as Azure AD, AWS Identity and Access Management (IAM), and Okta to name a few. Adding directory integration with common directory services is a great way to get customers on board and working securely within user applications.
Data Retention Controls	
Automation	From a security standpoint, automation can be a huge force multiplier to the effectiveness of an application. But there are a couple of points to be aware of and consider when automating processes and tasks.
Sessions	It is important that when an administrator modifies, deletes or removes an account that user has the added feature of cutting off active sessions with that deleted user account. When an account is deleted or has a password changed, all existing sessions should, therefore, be deleted immediately.
Monitor Account Activity	

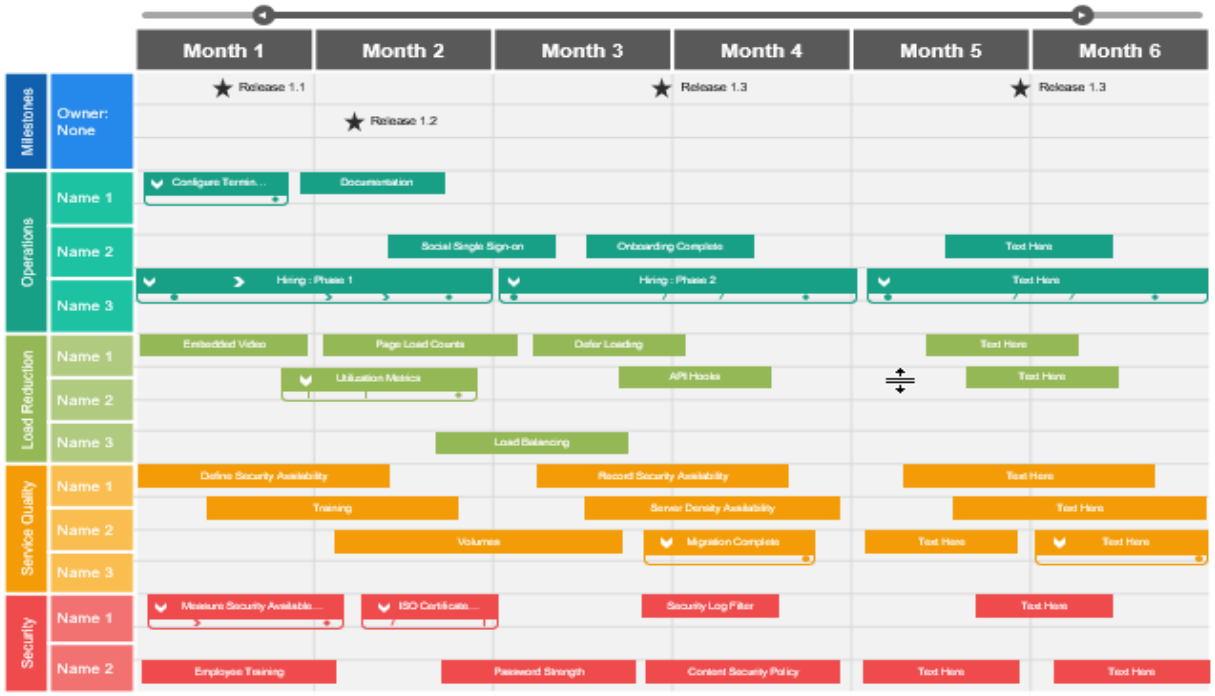
Artifacts Support for Security Strategy

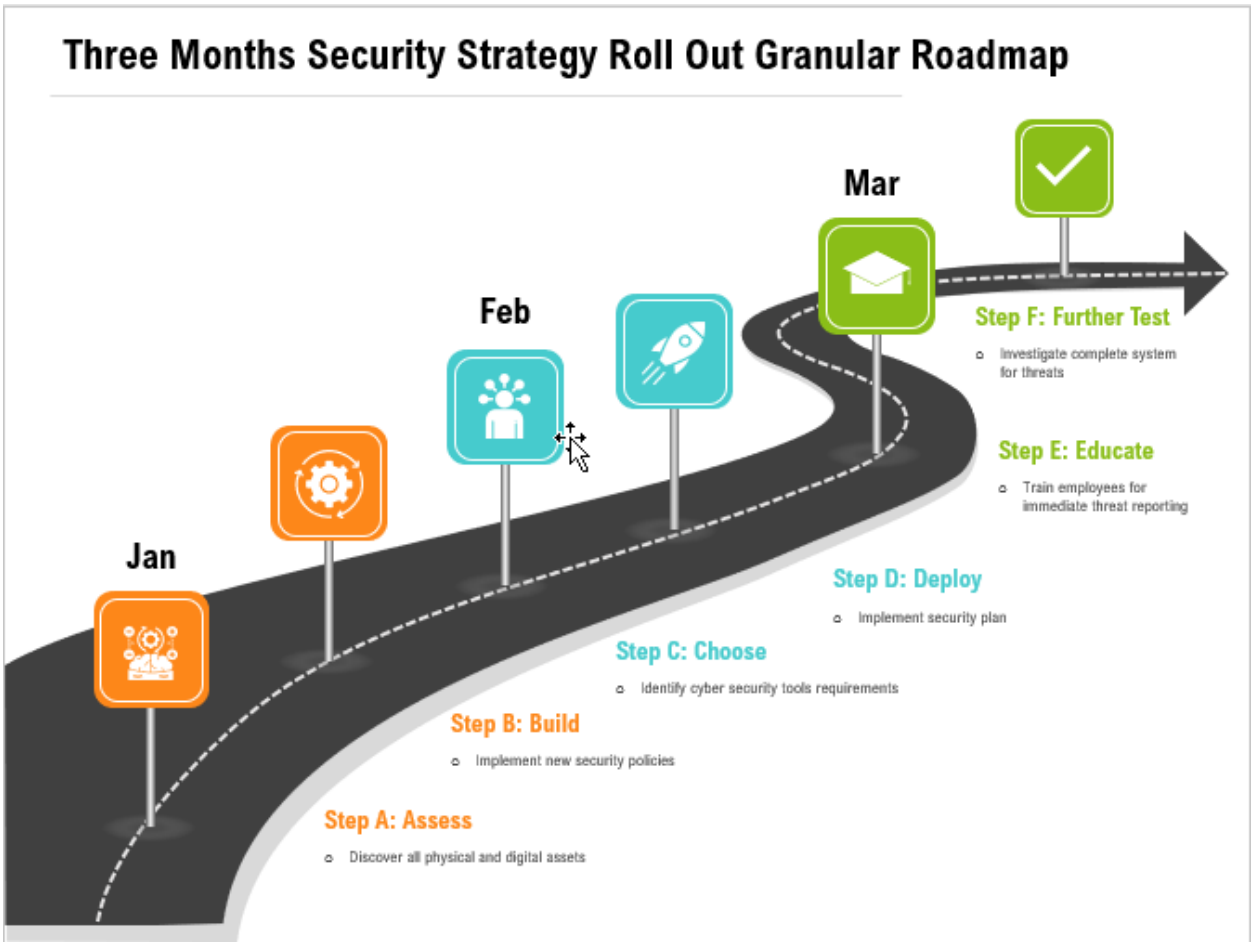


Half Yearly Security Strategy Program Maturity Roadmap According to Roadmap Cost



Six Months Technology Security Service Quality According to Owners




Three Months Security Strategy Roll Out Granular Roadmap
Jan
Feb
Mar
Step A: Assess
Discover all physical and digital assets
Step B: Build
Implement new security policies
Step C: Choose
Identify cyber security tools requirements
Step D: Deploy
Implement security plan
Step E: Educate
Train employees for immediate threat reporting
Step F: Further Test
Investigate complete system for threats

Addressing Different Security Priorities at Organization According to Strategy Selection