SECURITY TEAM

PALO IT Cyber Security Services

PALO IT

Andres Fernandez

CISO

Security strategy : Principle

Cybersecurity is not the business.

Ṹt should be **allowing the business** to make risk-informed decisions while delivering value to customers and stakeholders

What areas do we cover?

	AppSec	Physical Infrastructure	Cloud Infrastructure	Policies and Regulations Compliance
Product Level	✓ DevSecOps	✓ Routers ✓ Host firewall ✓ CCTV ✓ Fingerprint	✓ AWS ✓ GCP ✓ Azure ✓ RedHat, IBM	✓ PDPA/ GDPR ✓ TRM (MAS) ✓ ISO 27001 ✓ SOC 2 ✓ CIS ✓ NIST 800-53
Enterprise Level		✓ End-user devices (laptops, mobile)	✓ o365 ✓ SharePoint	

End-to-end cybersecurity protection

Where a Community of (Security) Practices, Integrates with the team and takes care of the security posture of the project, growing security champions.

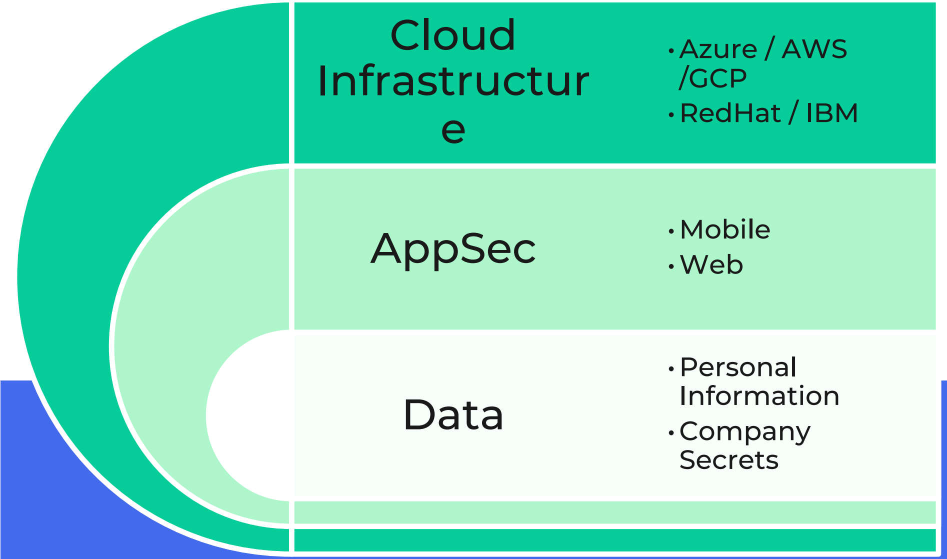
PALO IT

End-to-end cybersecurity protection

What do you get?

End to end Security in all project’s stages

People, technology, processes



Cloud Infrastructure
- Azure / AWS /GCP
- RedHat / IBM

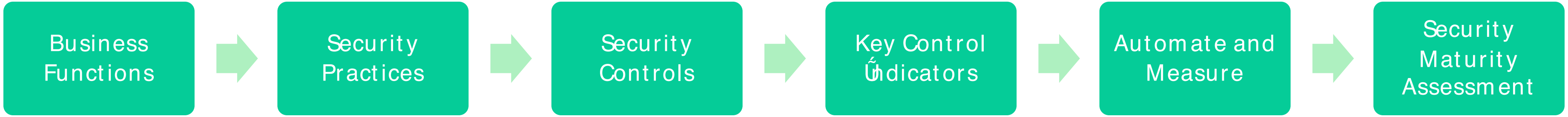
AppSec
- Mobile
- Web

Data
- Personal Information
- Company Secrets

Cybersecurity Maturity Assessment	Vulnerability assessment	Incidence response
Compliance with regulations	Zero-trust architecture	Risk assessment
Cybersecurity Strategy & Roadmap	Automation with DevSecOps	Clear KPIs reports

End-to-end cybersecurity protection

How do we do it?

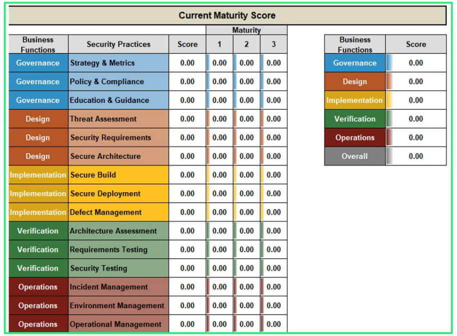


Business Functions → Security Practices → Security Controls → Key Control Ǘndicators → Automate and Measure → Security Maturity Assessment

OWASP Software Assurance Maturity Model (SAMM)

Critical Security Controls v8 (CǗS)

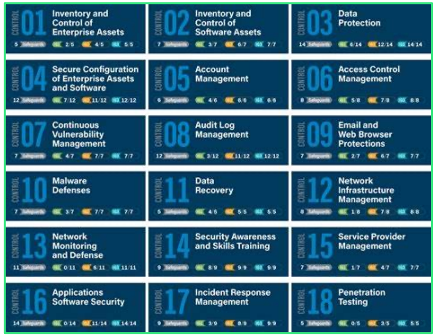
NǗST approach for DevSecOps, and security operations



Current Maturity Score

Business Functions	Security Practices	Score	Maturity 1	2	3
Governance	Strategy & Metrics	0.00	0.00	0.00	0.00
Governance	Policy & Compliance	0.00	0.00	0.00	0.00
Governance	Education & Guidance	0.00	0.00	0.00	0.00
Design	Threat Assessment	0.00	0.00	0.00	0.00
Design	Security Requirements	0.00	0.00	0.00	0.00
Design	Secure Architecture	0.00	0.00	0.00	0.00
Implementation	Secure Build	0.00	0.00	0.00	0.00
Implementation	Secure Deployment	0.00	0.00	0.00	0.00
Implementation	Defect Management	0.00	0.00	0.00	0.00
Verification	Architecture Assessment	0.00	0.00	0.00	0.00
Verification	Requirements Testing	0.00	0.00	0.00	0.00
Verification	Security Testing	0.00	0.00	0.00	0.00
Operations	Incident Management	0.00	0.00	0.00	0.00
Operations	Environment Management	0.00	0.00	0.00	0.00
Operations	Operational Management	0.00	0.00	0.00	0.00

Business Functions	Score
Governance	0.00
Design	0.00
Implementation	0.00
Verification	0.00
Operations	0.00
Overall	0.00



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

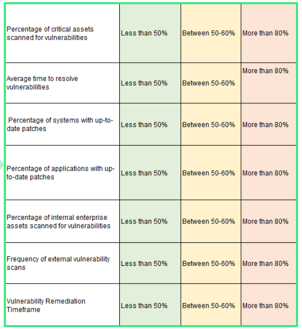
CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

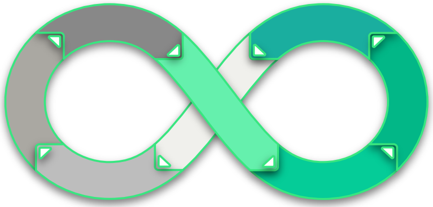
CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5



Percentage of critical assets scanned for vulnerabilities	Less than 50%	Between 50-60%	More than 80%
Average time to resolve vulnerabilities	Less than 50%	Between 50-60%	More than 80%
Percentage of systems with up-to-date patches	Less than 50%	Between 50-60%	More than 80%
Percentage of applications with up-to-date patches	Less than 50%	Between 50-60%	More than 80%
Percentage of internal enterprise assets scanned for vulnerabilities	Less than 50%	Between 50-60%	More than 80%
Frequency of external vulnerability scans	Less than 50%	Between 50-60%	More than 80%
Vulnerability Remediation Timeframe	Less than 50%	Between 50-60%	More than 80%



Information Classification: CONFIDENTIAL (sensitive business information, the level of protection is dictated by legal agreements)

Secure AI Environments

What problem are we trying to solve?

- Data leakage. Training sensitive data could be leaked to unauthorized users.
- Vulnerable Infrastructure. External actors could break into the environment due to account takeover or vulnerable architecture.

Example Scenario

Email triage system so that customers with some of the common queries (such as a change of home address) could be automatically directed towards a web form that would resolve their query

Incoming emails

Classified according to customer intent

Those customers who can solve their problem with a simple web form are directed to the correct form.

Compliance Problems

- The users **have not consented** for their emails to be stored. I cannot store it indefinitely. It must be deleted.

- Under the GDPR's **right to be forgotten**, a user can request that the organization delete all of their personal data. If a user were to submit such a request, **how would I track down all places** that the personal data has permeated to in the machine learning pipeline? It must be possible to trace all copies of an email in all datasets.

- Can any **sensitive data be reproduced from the model**? For example, if a customer's email address was stored in a model as a word in its vocabulary. We must take care to ensure that nobody could reconstruct any sensitive information from a trained model.

Solutions

Technique	Pros	Cons
1. Delete the dataset Once the machine learning model has been trained, the data scientist must delete the complete dataset.	if all data is truly deleted, then there is no way that the data can leak, and the “right to be forgotten” is no longer an issue.	If the project were to resume in future, **you would need to re-annotate** a new dataset.
2. Anonymise (mask) data Process all emails using a data anonymization algorithm to remove names, addresses or other sensitive information	If no sensitive data goes anywhere near the machine learning model, it cannot remember anything it shouldn’t	What **remains may not be sufficient** to train an accurate machine learning model. Is difficult, time-consuming, and it is possible to accidentally leave a sensitive piece of information in
3. Store only IDs which can be used to reconstruct data (embeddings) Annotate the data and then delete it, storing only a hash or ID of the original information, so that the training data can be easily reconstructed but it is not stored in your machine learning system	The **training data can be re-built** provided the emails have not been deleted from the email server. This means that the machine learning project does not rely on any extra copies of data.	If a hacker got hold of your hashed database as well as a database of email addresses from another company, they could hash all those email addresses and cross check them against your database and reconstruct the original email addresses.

Solutions

	Pros	Cons
4. Encrypt or transform the data and work on it in encrypted space (homomorphic encryption) Obfuscate a sensitive dataset in such a way, that the sensitive data can’t be reconstructed, but machine learning can still learn from it	A simple way of achieving the same result is to transform numeric fields using Principal Component Analysis. For example, a transformed value could be 2 * age + 1.5* salary + 0.9 * latitude, which would be very hard to map back to an individual due to the many-to-one nature of the transformation.	Homomorphic encryption is often very hard to do
5. Automated security and resilient. Automated AI driven chaos testing engineering with prompts inputs. Brute force prompts to ensure there is not way to retrieve sensitive data.		

Solutions

Technique	
Strengthen security measures in communication	In addition to ensuring that no data is copied unnecessarily, or checked into repositories, there are other routine security measures which need to be taken in the case of sensitive training data. For example, any API endpoints must be secured with SSL and HTTPS, and you should not share data over third-party services such as GitHub or Gmail.
Keep sensitive data in a silo and don't allow data scientists to access it directly, but let them experiment on it by submitting jobs to a secure platform	It is also possible to keep the sensitive data in a safe repository where researchers cannot access it directly, but they can submit experiments to it and perform statistical tests
Strong access control	
Zero trust architecture	

End-to-end cybersecurity protection

Secure System Development Lyfecycle (SDLC)

Automated security

Phase	Implementation
Plan	Threat modelling
Design	Follow zero trust security practices
Code	Source Code Review for every pull request • IDE review integration
Build	**Static security test** Static Application Security Testing (SAST) tools to detect security vulnerabilities in proprietary code by scanning an application’s code for flaws that are indicative of security vulnerabilities while the code is still in a static/non-running state • Snyk rules: Security Rules used by Snyk Code - Snyk User Docs
Build	**Secrets scanning** • Snyk rules: Security Rules used by Snyk Code - Snyk User Docs
Build	**Software Composition Analysis (SCA)** We automate the entire process of managing open-source components, including selection, alerting on any security or compliance issues, or even blocking them from the code. • Image scanning - Snyk • Open-Source Dependencies scanning - Snyk
Build	**Break the build analysis** • Every Pull Request triggers security test • PR only allowed to merge if all security gates are green

Implementation and Improvement

Automated security

Phase	Implementation
Test	**Penetration Testing** Pen tests are either performed annually or when major releases. Includes a follow-up regression testing to validate that the mitigating actions are implemented effectively.
Test	**Certificate on a web server** Test secure strength of certificates
Release	**Infrastructure configuration** Implement automated tools based on the chosen technologies to implement security configuration baselines such as CIS controls.
Release	**Legitimate artifacts are deployed** Sign the generated artifact and validate signature before deploying into the target environment.
Operate	**Incident Response** Defined process to define the incidence response lifecycle
Operate	**Change Management** Defined process to evaluate risk assessment when making changes to prevent adding vulnerabilities
Operate	**Patch Management** Automated tooling are implemented to detect available patches
Monitor	**SIEM** Correlate all logs in a central location to establish normal and abnormal behaviors and create alerts.
Monitor	**Vulnerability Assessment** A vulnerability assessment report is used to take appropriate risk mitigation actions and make risk-based decisions regarding the continued operations of the system and

PALO IT is DPTM (Data Protection Trustmark) Certified Organization

Responsible Data Protection Practices in our Development

- The DPTM (Data Protection Trustmark), certifies the soundness of our data protection policies and practices.
- In today’s data-driven digital economy, consumer trust is essential to deploy innovative technology that makes use of personal data to deliver more personalised services.
- You can rest assured that an organisation certified with the DPTM has put in place responsible data protection practices and will take better care of your personal data.

DATA PROTECTION
ASSURED