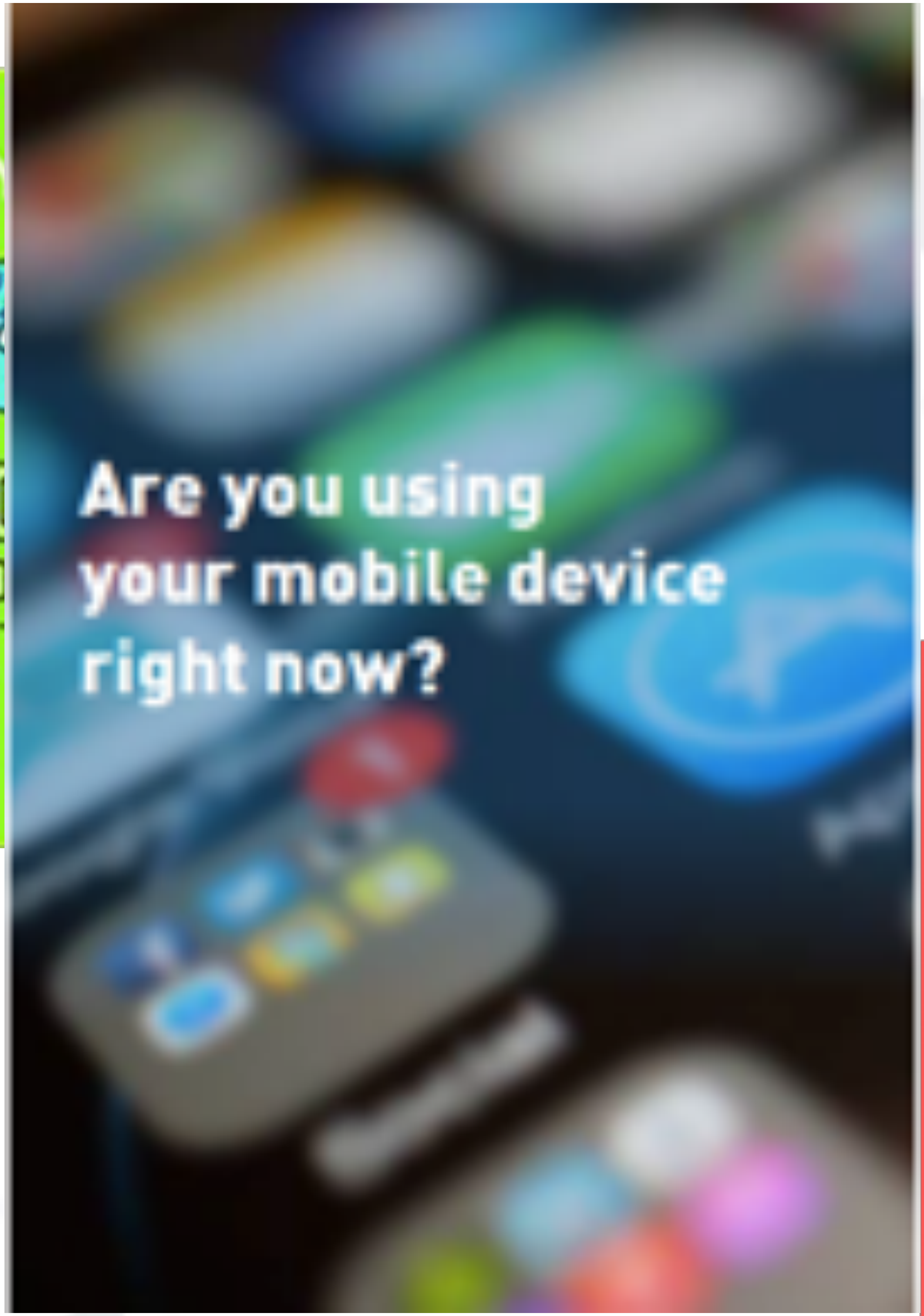
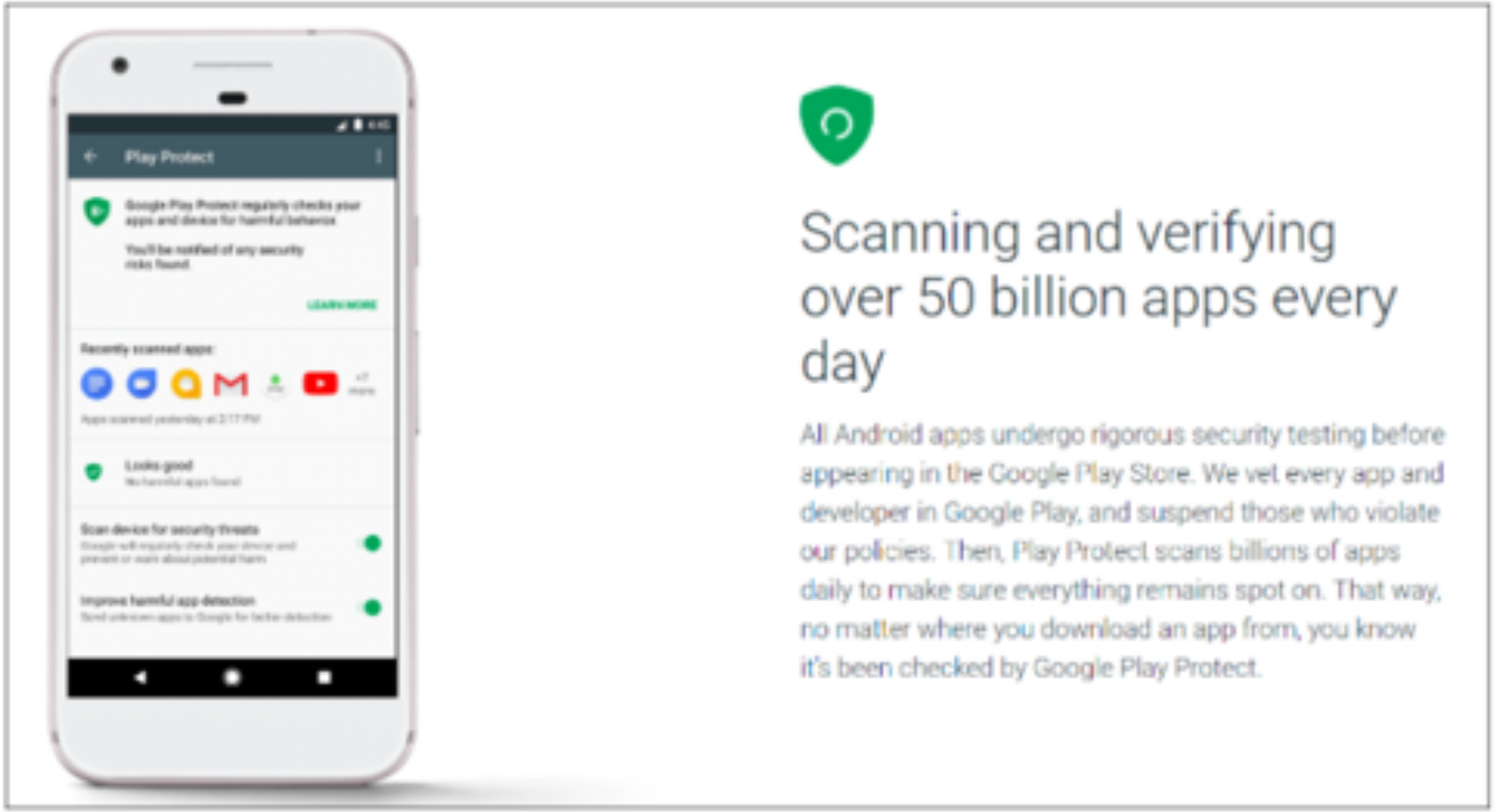
CSA APAC cloud security alliance®
ASIA PACIFIC REGION

Your Mobile App – At Full or Half MAST?

Ekta Mishra
APAC Membership Director &
Country Manager - India

HOW SAFE IS Y


Are you using
your mobile device
right now?



Play Protect

Google Play Protect regularly checks your apps and device for harmful behavior

You'll be notified of any security risks found

LEARN MORE

Recently scanned apps:

+7 more

Apps scanned yesterday at 2:17 PM

Looks good
No harmful apps found

Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm

Improve harmful app detection
Send unknown apps to Google for better detection

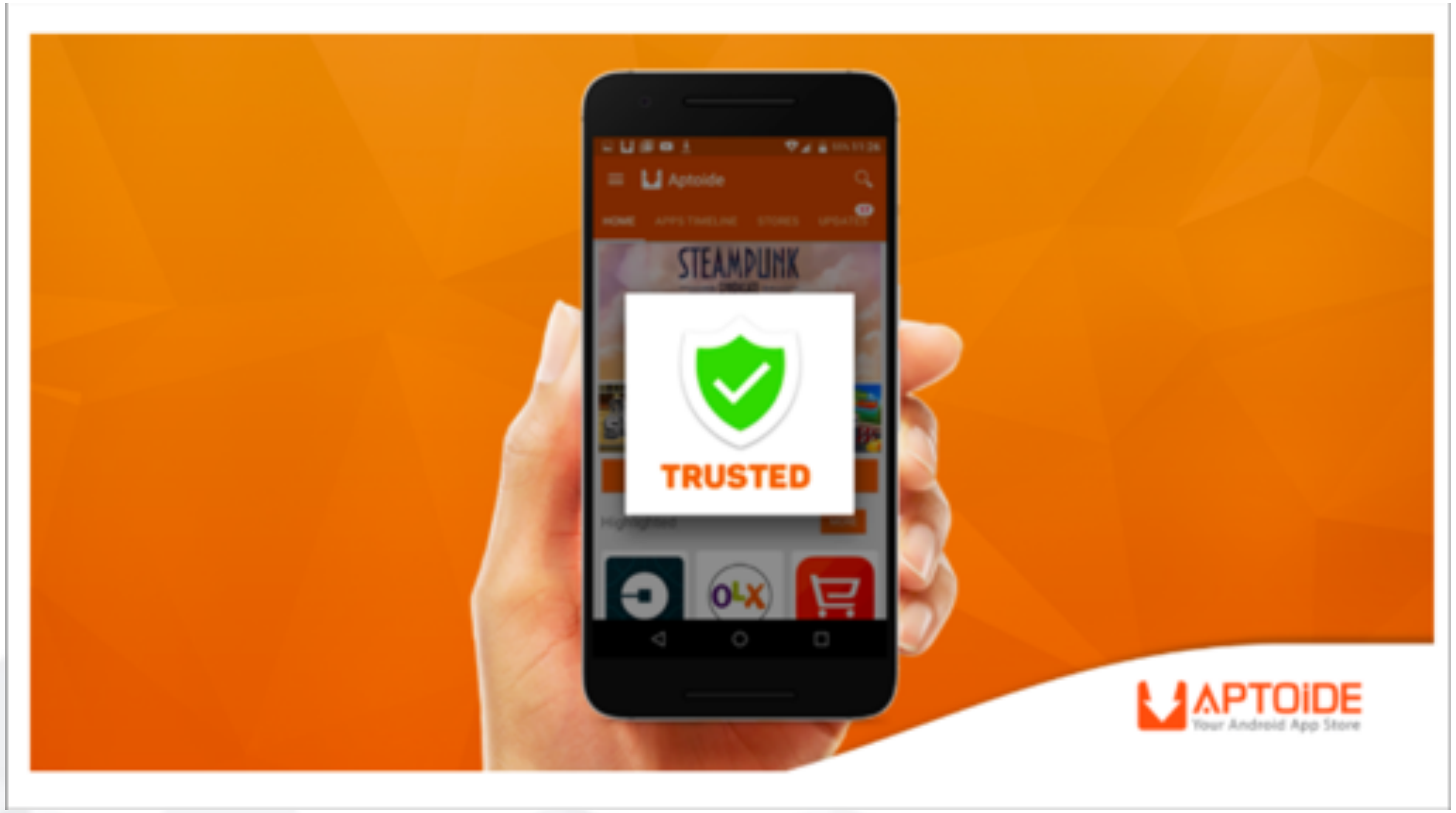
Scanning and verifying over 50 billion apps every day

All Android apps undergo rigorous security testing before appearing in the Google Play Store. We vet every app and developer in Google Play, and suspend those who violate our policies. Then, Play Protect scans billions of apps daily to make sure everything remains spot on. That way, no matter where you download an app from, you know it's been checked by Google Play Protect.

Google Play

Play Protect's Malware Scanner Keeps Your Phone Virus-Free

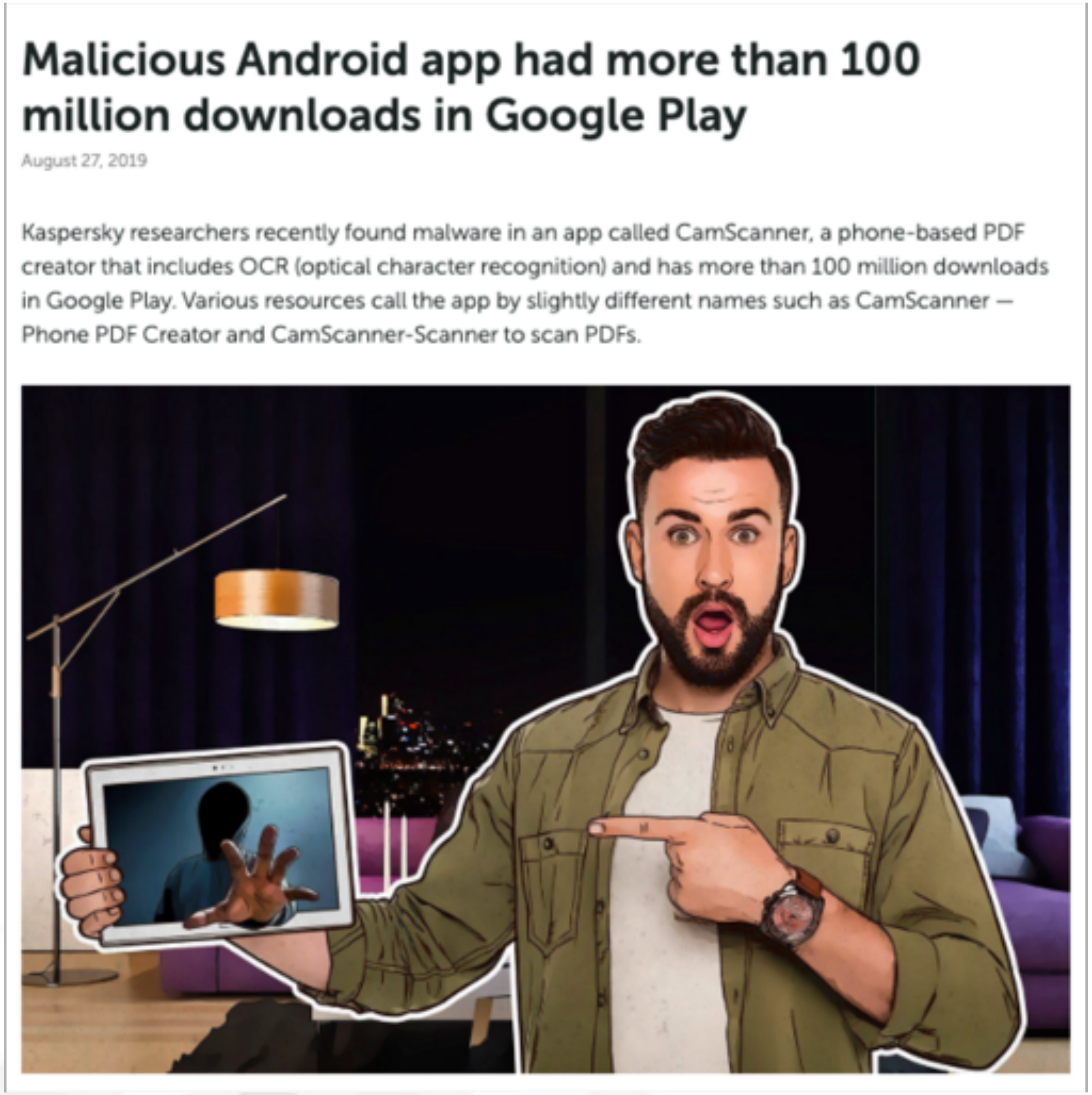
Is Aptoide Safe?



"Aptoide has made the protection of its users one of its key concerns - That's why we have developers continuously developing and upgrading Aptoide Anti-Malware System".

Six broad types of apps that can compromise your smartphone

1. Data Stealer
2. Premium Service Abuser
3. Click Fraudster
4. Malicious Downloader
5. Spying tools
6. Rooter

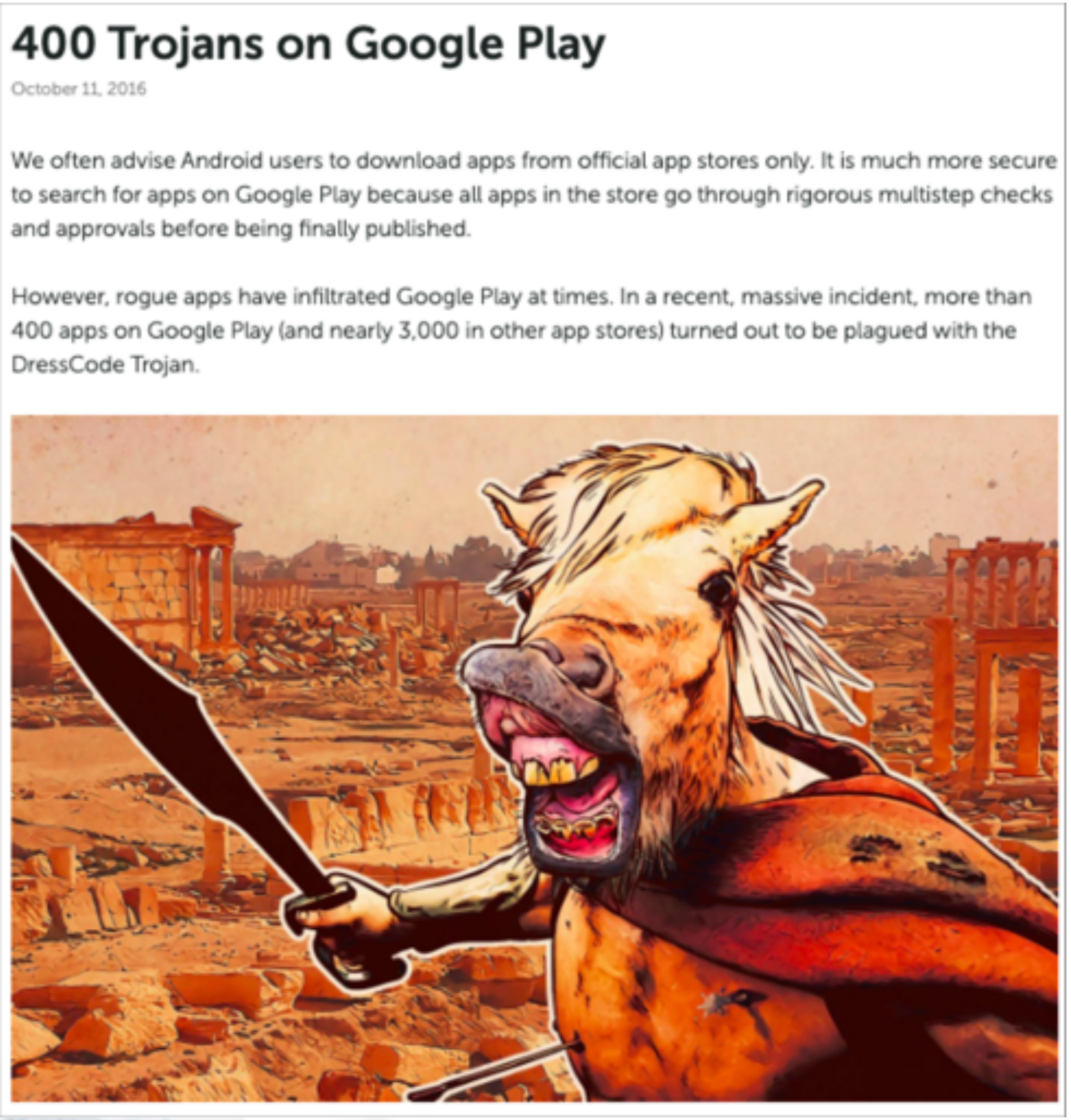


Malicious Android app had more than 100 million downloads in Google Play

August 27, 2019

Kaspersky researchers recently found malware in an app called CamScanner, a phone-based PDF creator that includes OCR (optical character recognition) and has more than 100 million downloads in Google Play. Various resources call the app by slightly different names such as CamScanner — Phone PDF Creator and CamScanner-Scanner to scan PDFs.

Source : https://www.kaspersky.co.in/blog/camscanner-malicious-android-app/16595/



400 Trojans on Google Play

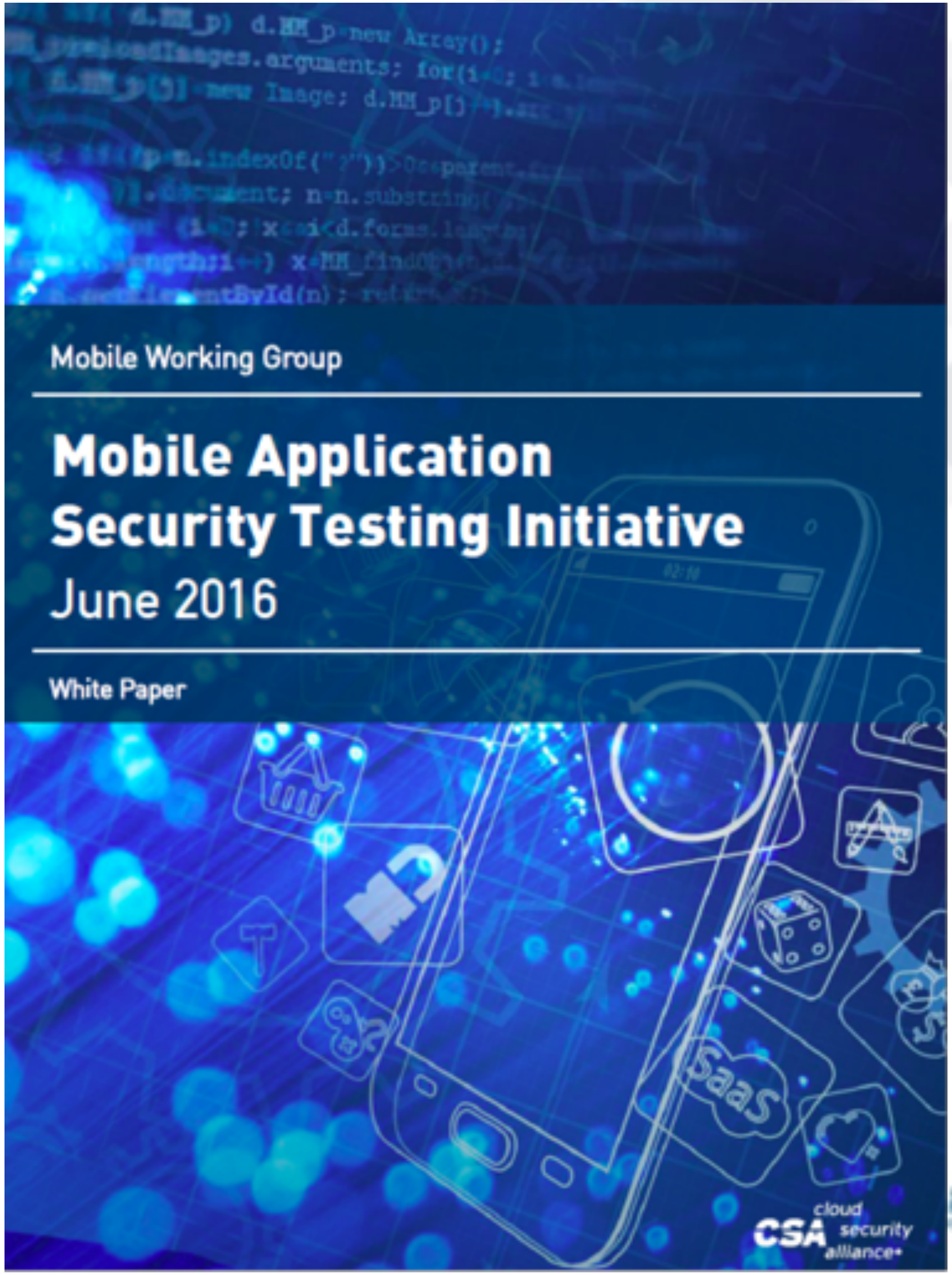
October 11, 2016

We often advise Android users to download apps from official app stores only. It is much more secure to search for apps on Google Play because all apps in the store go through rigorous multistep checks and approvals before being finally published.

However, rogue apps have infiltrated Google Play at times. In a recent, massive incident, more than 400 apps on Google Play (and nearly 3,000 in other app stores) turned out to be plagued with the DressCode Trojan.

Source :
https://www.kaspersky.com/blog/dresscode-android-trojan/13219/

How can we manage the security of mobile applications?



Mobile Working Group

Mobile Application Security Testing Initiative

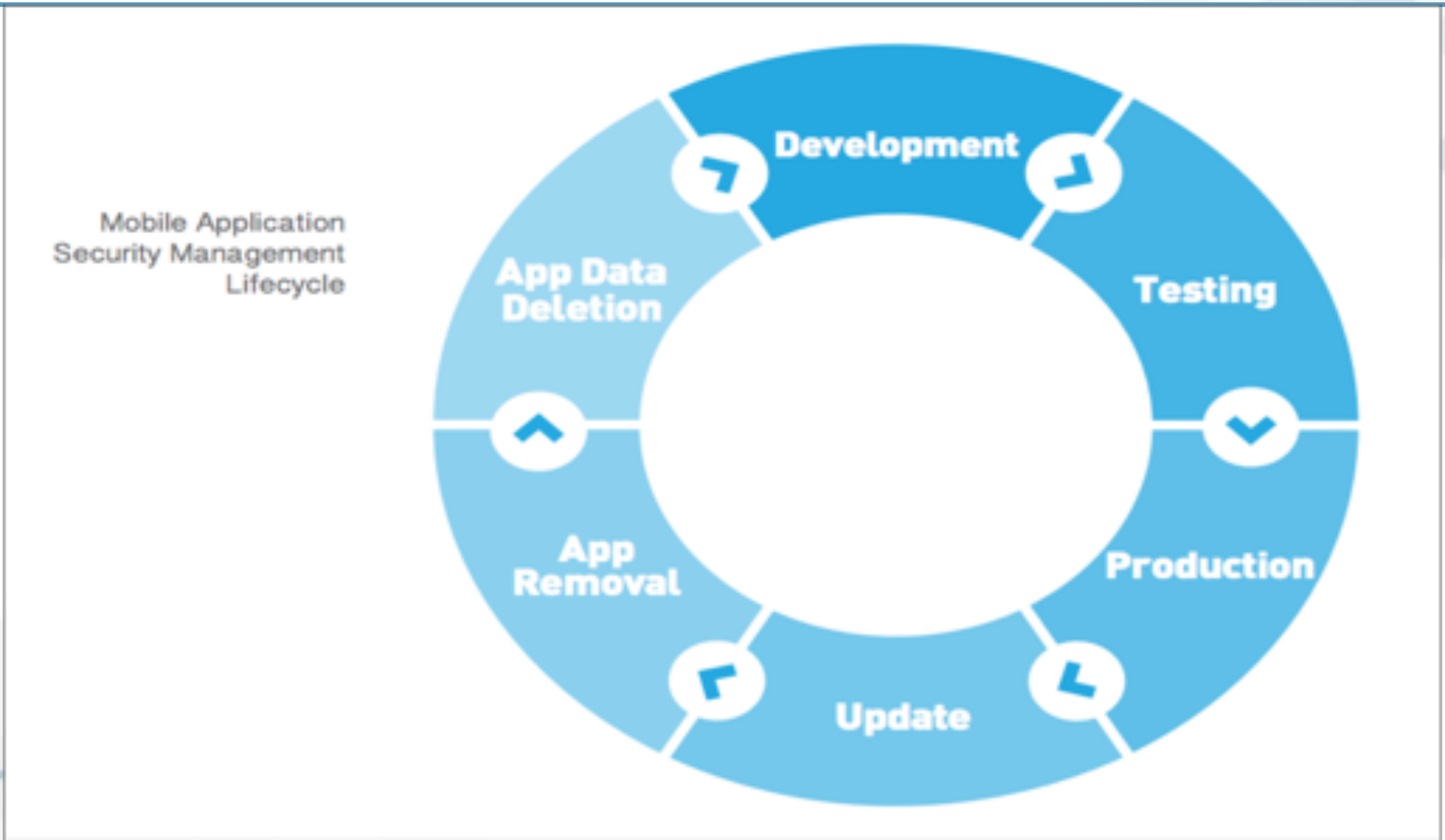
June 2016

White Paper

CSA cloud security alliance®

Mobile Application Security Management Lifecycle

How can we manage the security of mobile applications?



Development

- Check whether kit version management is conducted as documented.

- Check whether program code origin assurance has been done by designated personnel.

- Check whether continuous security vetting management is conducted during various phases within the application development lifecycle.

Testing

- Check whether a standardized security vetting guideline is applied.

- Check whether vetting result feedback has been delivered to the system for future development revisions or other testing processes.

Production

- Perform version control during application production.
- Make sure application specifications follow the rules given by public markets such as Apple App store & Google Play.
- Check whether assurance management of version control & content procedures are in place for in-house applications.

Update

- Check whether an internal revision process has been established.

- Check whether all revisions have fulfilled the update requirements established by public markets, such as App Store & Google Play.

Application Removal

- Verify whether additional services, such as advertisement identification & any future online payments, have been canceled.

- Make sure that these activities are recorded for future assurance.

Application Data Deletion

- Check whether the data is completely erased from the device after an application has been uninstalled.

- Check whether there is a mechanism that will inform the cloud administrator about any application data that may remain.

CSA Mobile Application Security Testing Scheme

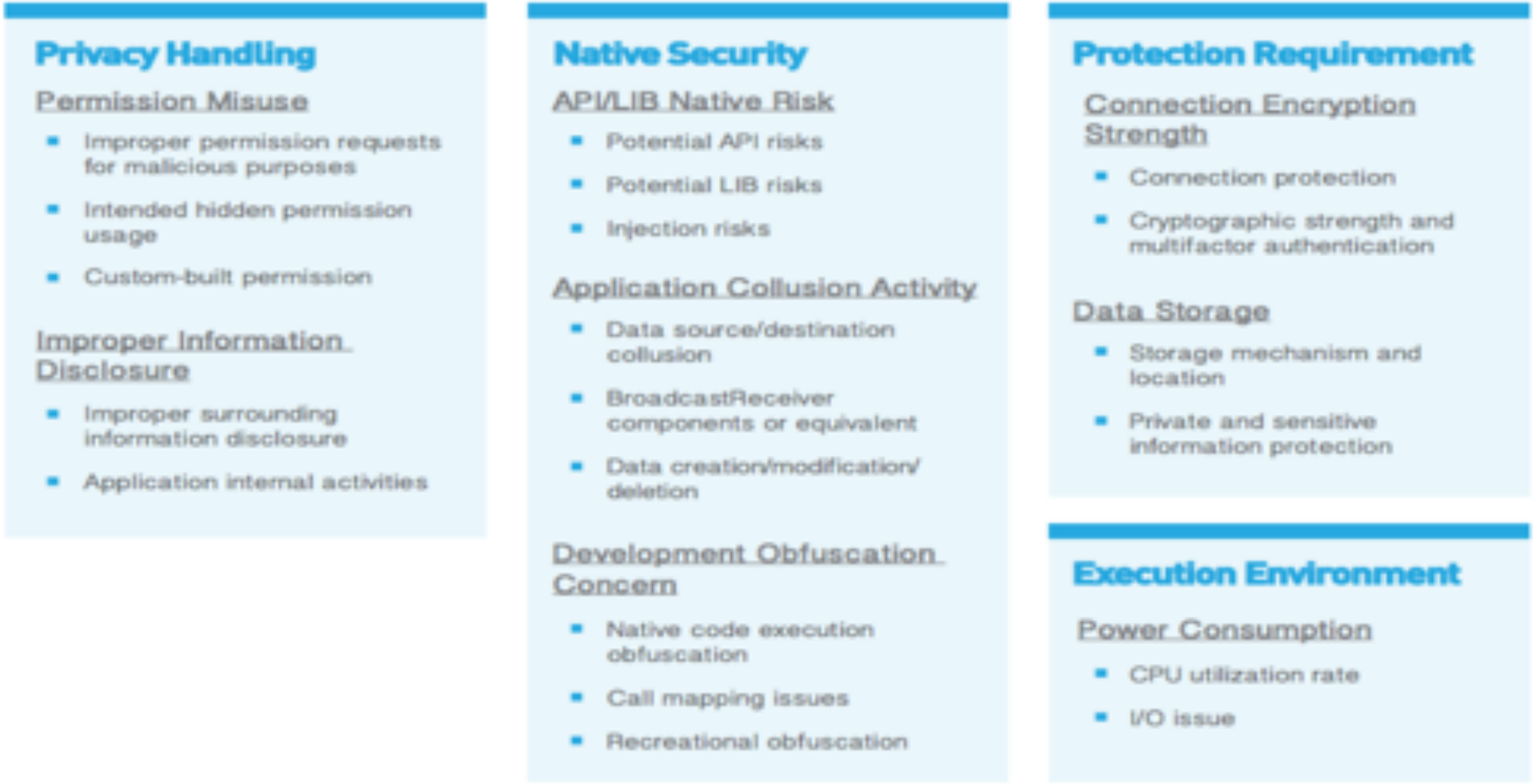
CSA Mobile Application Security Testing Scheme

- **Vetting with source code available**
  - Conducted either by the use of code review tools or by manual-source code reviews

- **Vetting without source code available**
  - Conducted vetting tests against files such as iPAs or APKs

- **Static & Dynamic**

Mobile Application Security Requirements



Privacy Handling

Permission Misuse

- Improper permission requests for malicious purposes
- Intended hidden permission usage
- Custom-built permission

Improper Information Disclosure

- Improper surrounding information disclosure
- Application internal activities

Native Security

API/LIB Native Risk

- Potential API risks
- Potential LIB risks
- Injection risks

Application Collusion Activity

- Data source/destination collusion
- BroadcastReceiver components or equivalent
- Data creation/modification/ deletion

Development Obfuscation Concern

- Native code execution obfuscation
- Call mapping issues
- Recreational obfuscation

Protection Requirement

Connection Encryption Strength

- Connection protection
- Cryptographic strength and multifactor authentication

Data Storage

- Storage mechanism and location
- Private and sensitive information protection

Execution Environment

Power Consumption

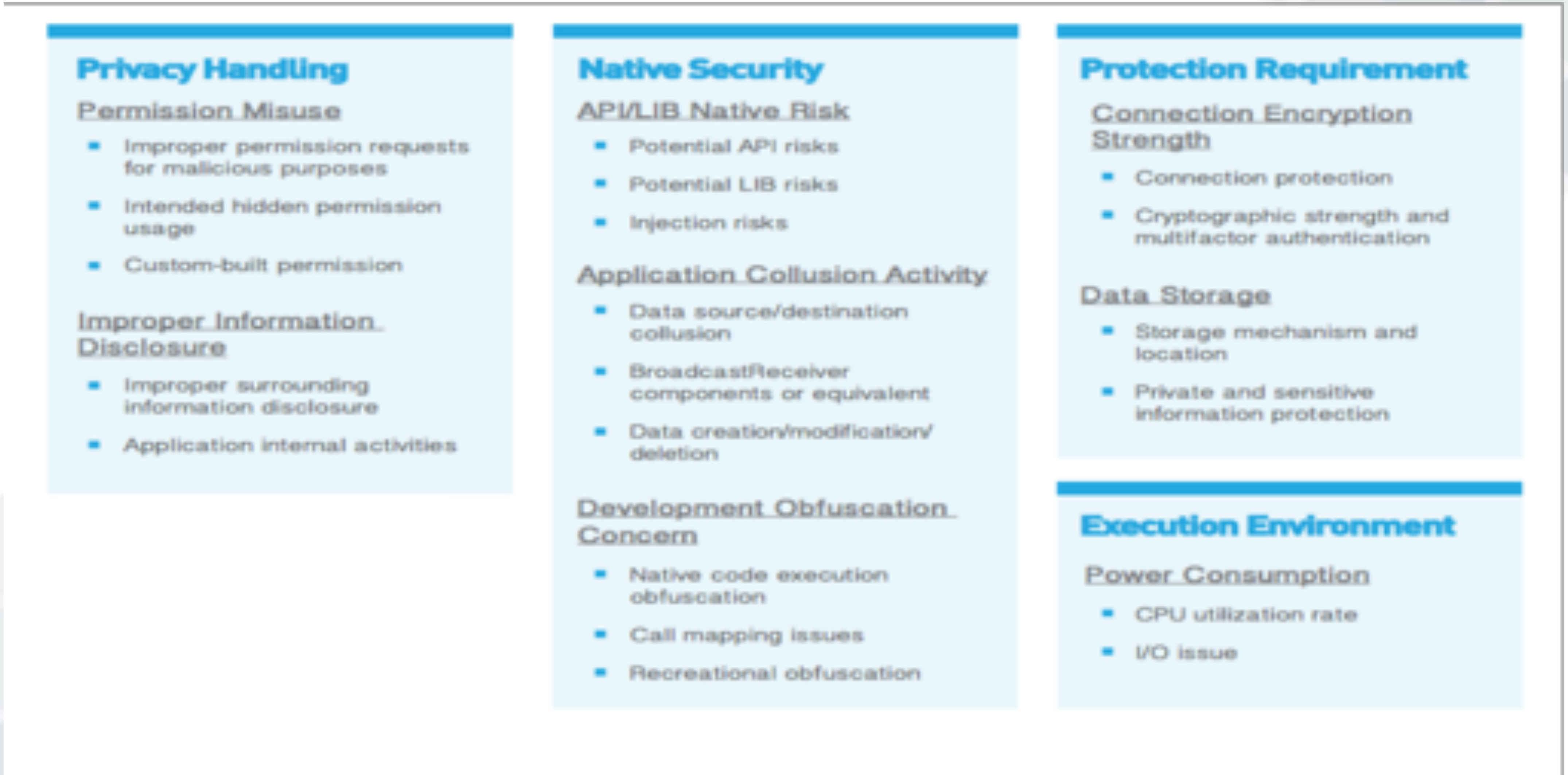
- CPU utilization rate
- I/O issue

Privacy Handling

- **Permission Misuse**
  - Improper permission requests for malicious purposes
  - Intended hidden permission usage
  - Custom-built permission

- **Improper Information Disclosure**
  - Improper surrounding information disclosure
  - Application internal activities

Mobile Application Security Requirements



Privacy Handling

Permission Misuse

- Improper permission requests for malicious purposes
- Intended hidden permission usage
- Custom-built permission

Improper Information Disclosure

- Improper surrounding information disclosure
- Application internal activities

Native Security

API/LIB Native Risk

- Potential API risks
- Potential LIB risks
- Injection risks

Application Collusion Activity

- Data source/destination collusion
- BroadcastReceiver components or equivalent
- Data creation/modification/ deletion

Development Obfuscation Concern

- Native code execution obfuscation
- Call mapping issues
- Recreational obfuscation

Protection Requirement

Connection Encryption Strength

- Connection protection
- Cryptographic strength and multifactor authentication

Data Storage

- Storage mechanism and location
- Private and sensitive information protection

Execution Environment

Power Consumption

- CPU utilization rate
- I/O issue

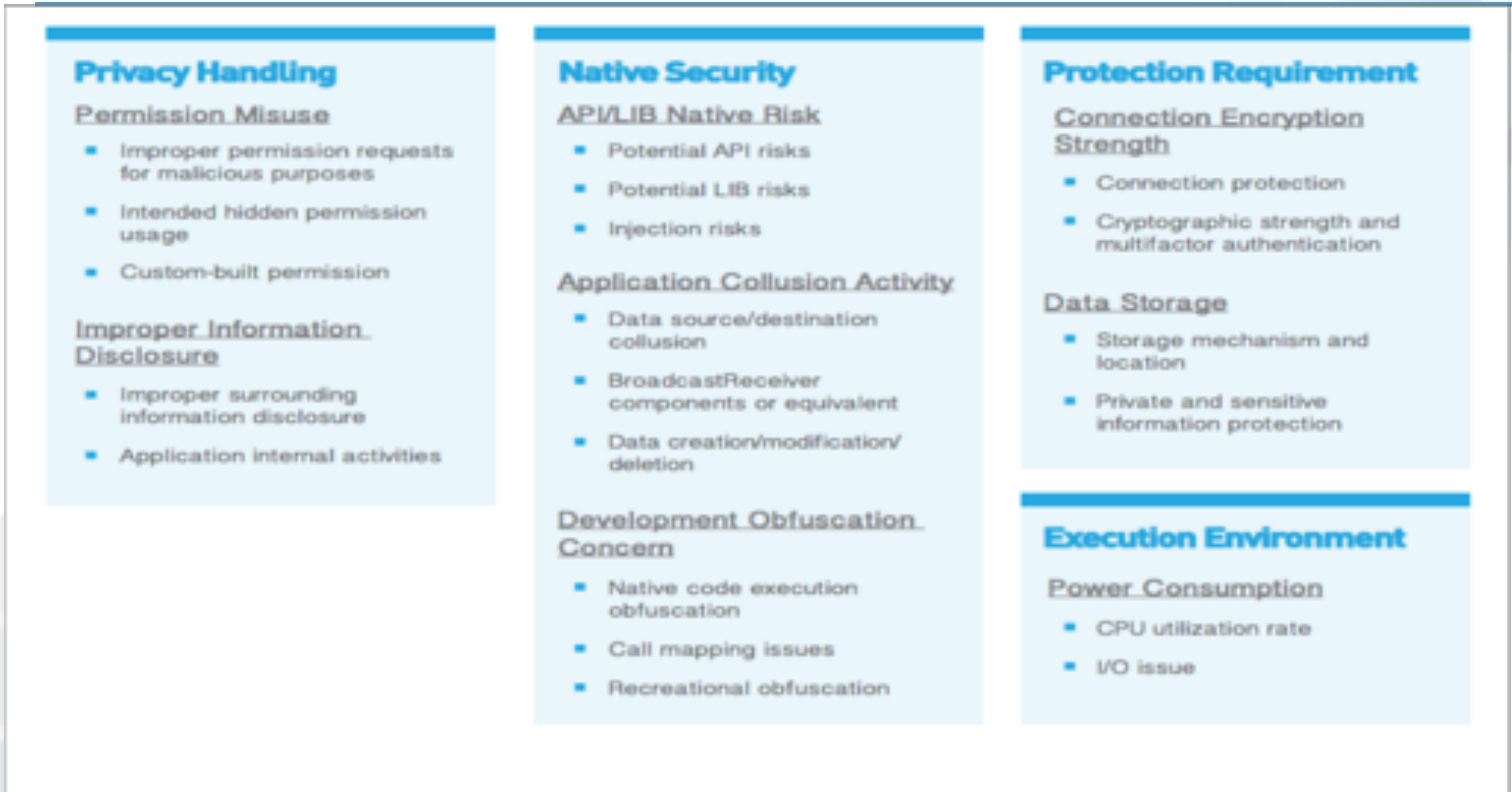
Native Security

- **API/LIB Native Risk**
  - Potential API risks
  - Potential LIB risks
  - Injection risks

- **Application Collusion Activity**
  - Data source/destination collusion
  - BroadcastReceiver components or equivalent
  - Data creation/modification/deletion

- **Development Obfuscation Concern**
  - Native code execution obfuscation
  - Call mapping issues
  - Recreational obfuscation

Mobile Application Security Requirements



Privacy Handling

Permission Misuse

- Improper permission requests for malicious purposes
- Intended hidden permission usage
- Custom-built permission

Improper Information Disclosure

- Improper surrounding information disclosure
- Application internal activities

Native Security

API/LIB Native Risk

- Potential API risks
- Potential LIB risks
- Injection risks

Application Collusion Activity

- Data source/destination collusion
- BroadcastReceiver components or equivalent
- Data creation/modification/ deletion

Development Obfuscation Concern

- Native code execution obfuscation
- Call mapping issues
- Recreational obfuscation

Protection Requirement

Connection Encryption Strength

- Connection protection
- Cryptographic strength and multifactor authentication

Data Storage

- Storage mechanism and location
- Private and sensitive information protection

Execution Environment

Power Consumption

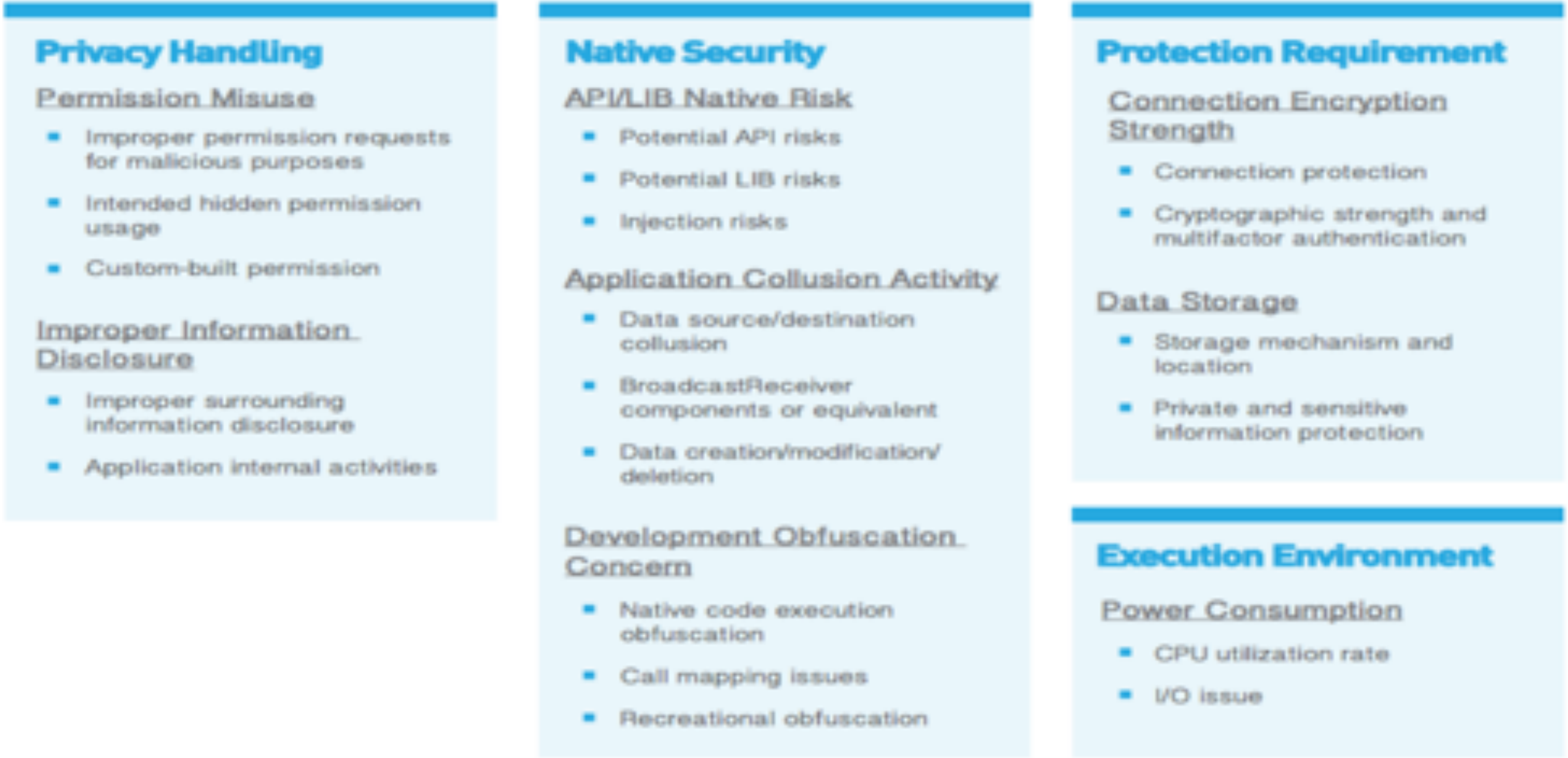
- CPU utilization rate
- I/O issue

Protection Requirement

- **Connection Encryption Strength**
  - Connection protection
  - Cryptographic strength & multifactor authentication

- **Data Storage**
  - Storage mechanism and location
  - Private & sensitive information protection

Mobile Application Security Requirements



Privacy Handling

Permission Misuse

- Improper permission requests for malicious purposes
- Intended hidden permission usage
- Custom-built permission

Improper Information Disclosure

- Improper surrounding information disclosure
- Application internal activities

Native Security

API/LIB Native Risk

- Potential API risks
- Potential LIB risks
- Injection risks

Application Collusion Activity

- Data source/destination collusion
- BroadcastReceiver components or equivalent
- Data creation/modification/ deletion

Development Obfuscation Concern

- Native code execution obfuscation
- Call mapping issues
- Recreational obfuscation

Protection Requirement

Connection Encryption Strength

- Connection protection
- Cryptographic strength and multifactor authentication

Data Storage

- Storage mechanism and location
- Private and sensitive information protection

Execution Environment

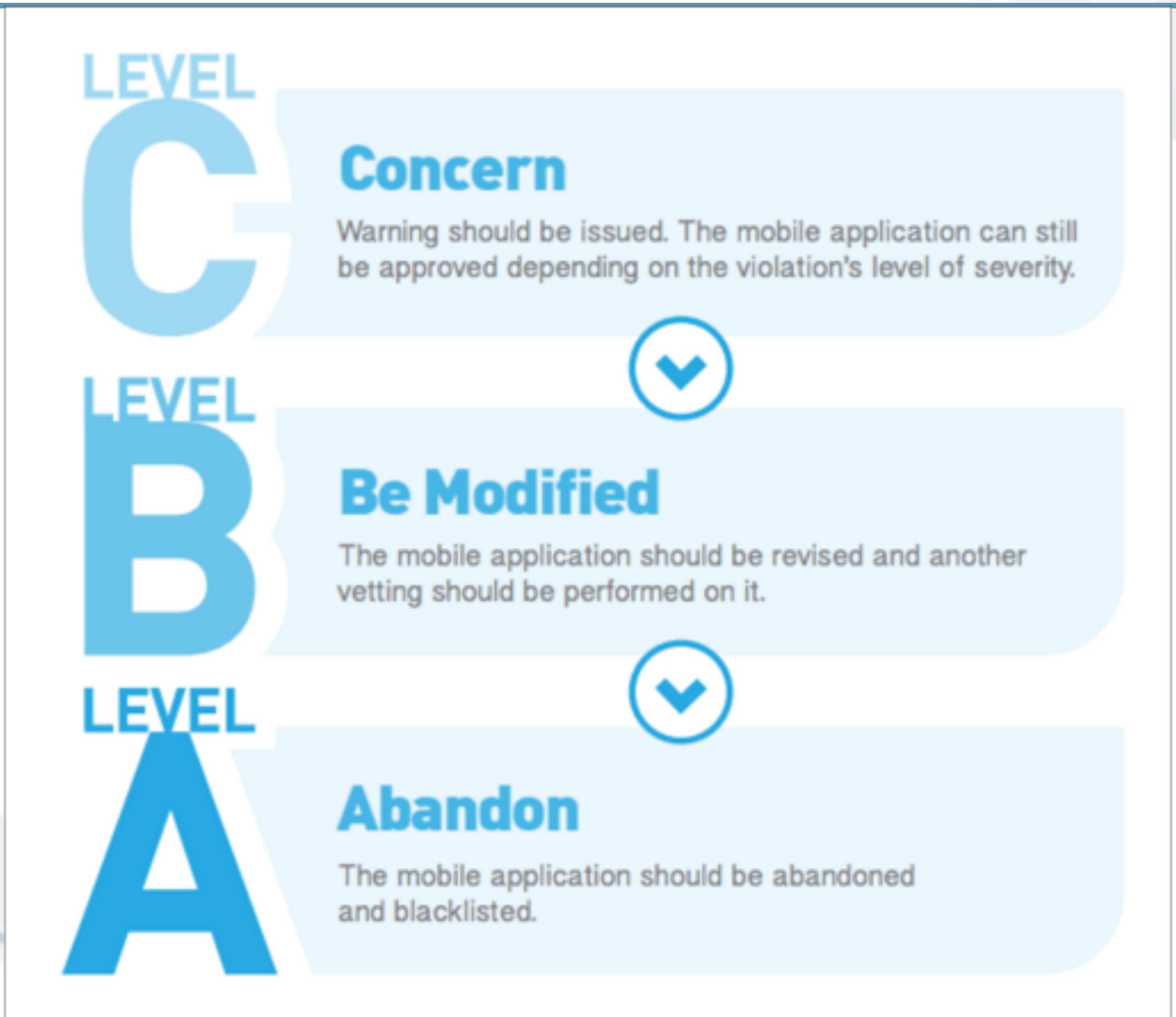
Power Consumption

- CPU utilization rate
- I/O issue

Execution Environment

- **Power Consumption**
  - Central processing unit (CPU) utilization rate
  - Input/output (I/O) issue

Content Classification and Rating



LEVEL C

Concern

Warning should be issued. The mobile application can still be approved depending on the violation's level of severity.

LEVEL B

Be Modified

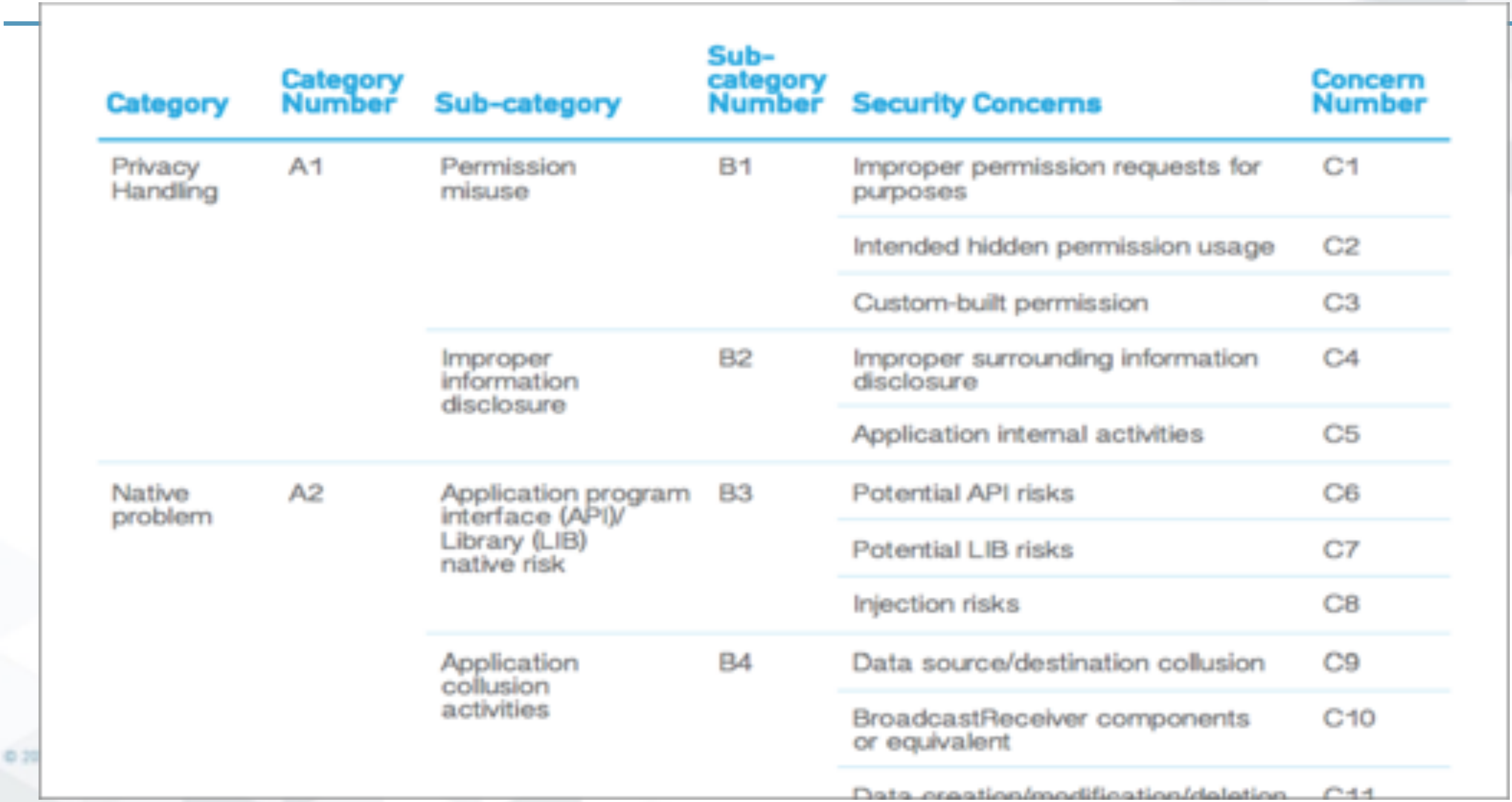
The mobile application should be revised and another vetting should be performed on it.

LEVEL A

Abandon

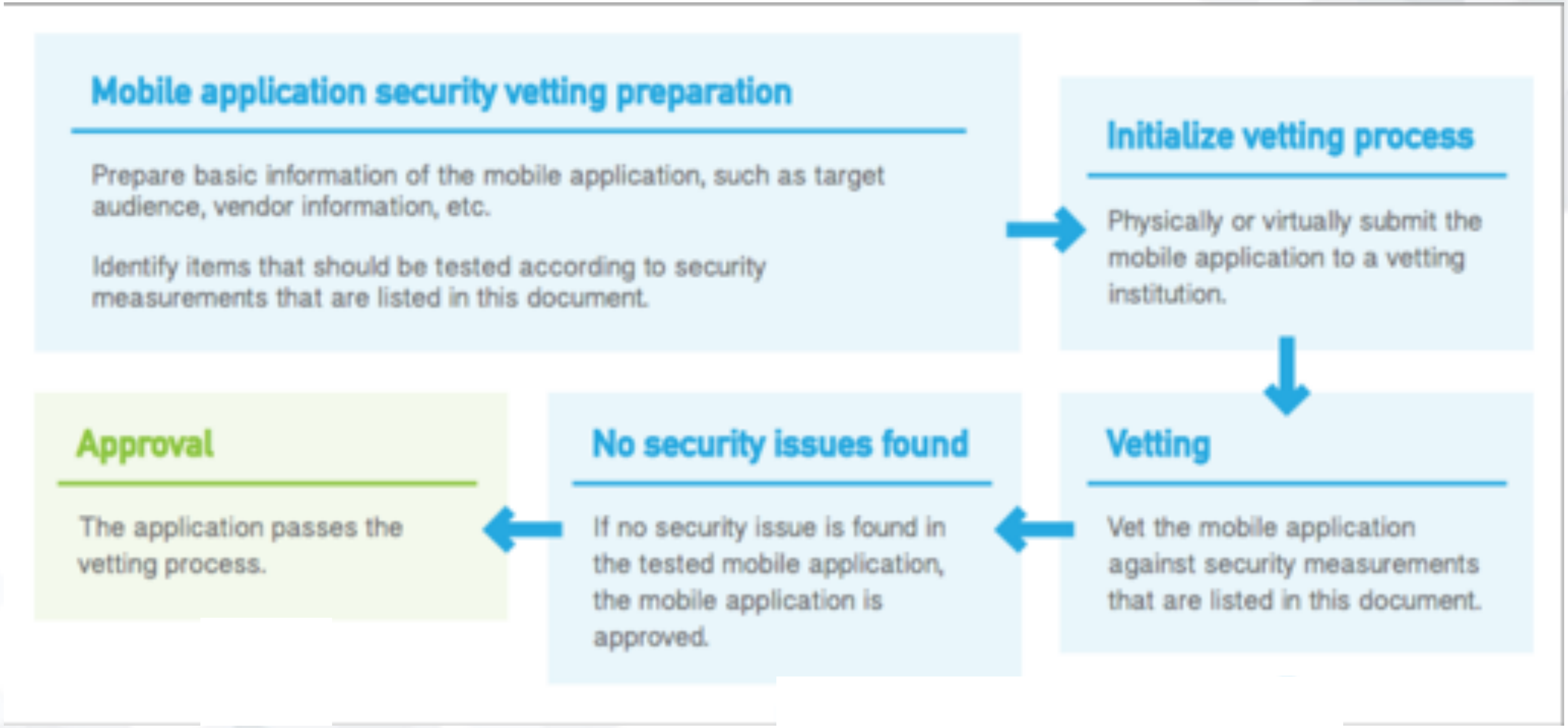
The mobile application should be abandoned and blacklisted.

Example of Mobile App Security Vetting Classification Scheme



Category	Category Number	Sub-category	Sub-category Number	Security Concerns	Concern Number
Privacy Handling	A1	Permission misuse	B1	Improper permission requests for purposes	C1
				Intended hidden permission usage	C2
				Custom-built permission	C3
		Improper information disclosure	B2	Improper surrounding information disclosure	C4
				Application internal activities	C5
Native problem	A2	Application program interface (API)/ Library (LIB) native risk	B3	Potential API risks	C6
				Potential LIB risks	C7
				Injection risks	C8
		Application collusion activities	B4	Data source/destination collusion	C9
				BroadcastReceiver components or equivalent	C10
				Data creation/modification/deletion	C11

Mobile Application Security Vetting Steps and Procedures



Mobile application security vetting preparation

Prepare basic information of the mobile application, such as target audience, vendor information, etc.

Identify items that should be tested according to security measurements that are listed in this document.

Initialize vetting process

Physically or virtually submit the mobile application to a vetting institution.

Vetting

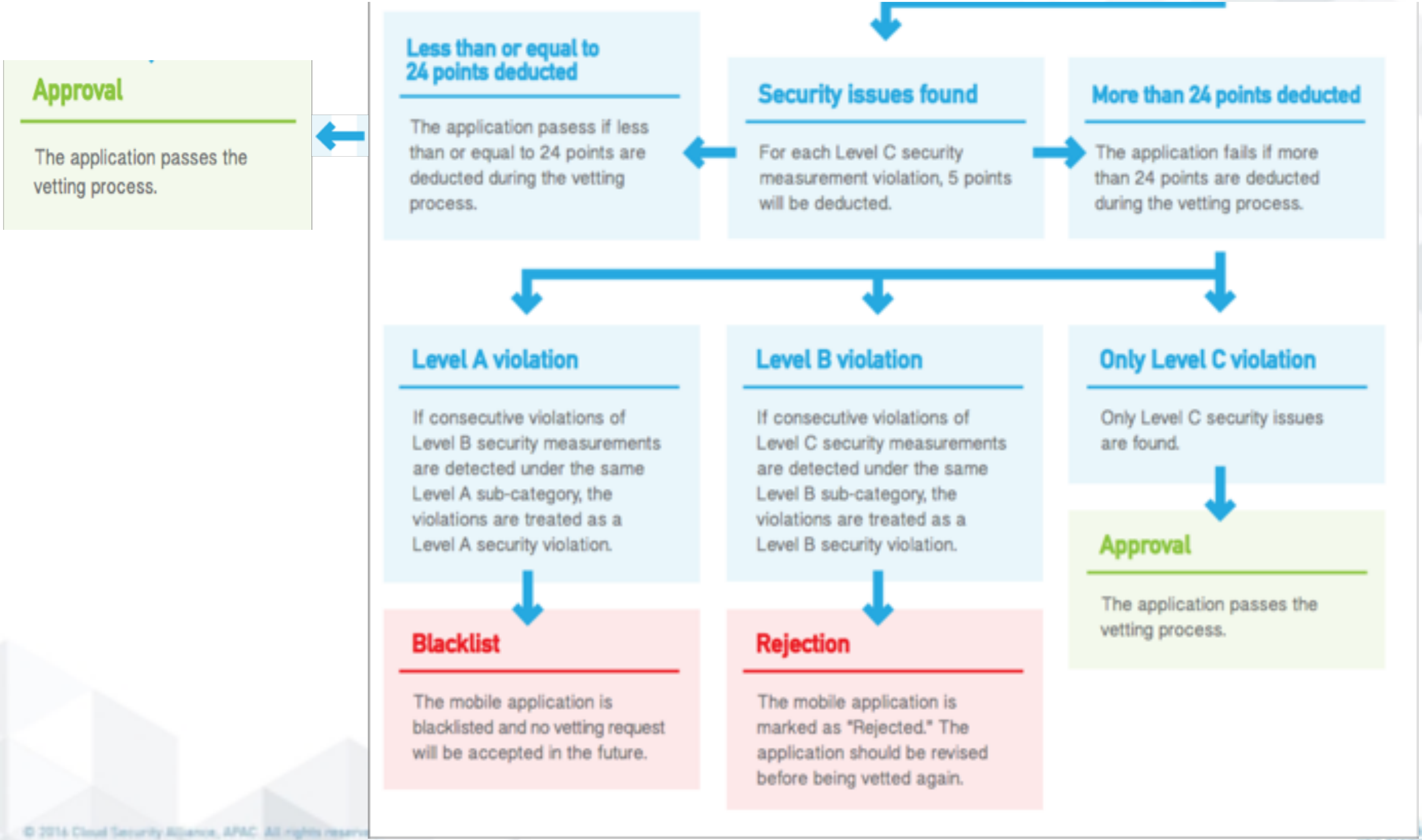
Vet the mobile application against security measurements that are listed in this document.

No security issues found

If no security issue is found in the tested mobile application, the mobile application is approved.

Approval

The application passes the vetting process.



Approval

The application passes the vetting process.

Less than or equal to 24 points deducted

The application pasess if less than or equal to 24 points are deducted during the vetting process.

Security issues found

For each Level C security measurement violation, 5 points will be deducted.

More than 24 points deducted

The application fails if more than 24 points are deducted during the vetting process.

Level A violation

If consecutive violations of Level B security measurements are detected under the same Level A sub-category, the violations are treated as a Level A security violation.

Level B violation

If consecutive violations of Level C security measurements are detected under the same Level B sub-category, the violations are treated as a Level B security violation.

Only Level C violation

Only Level C security issues are found.

Blacklist

The mobile application is blacklisted and no vetting request will be accepted in the future.

Rejection

The mobile application is marked as "Rejected." The application should be revised before being vetted again.

Approval

The application passes the vetting process.

In Progress

- Investigate and develop requirements for security of App Store
- Develop a mobile incident response handling procedure
- Develop a mobile forensic standard
- Investigate secure bootstrap for mobile phone

Deliverable: Mobile Application Vetting

- Align & map security controls under OWASP’s Mobile Security Testing Guide (MSTG) to the 2016 MAST whitepaper.

Potential Future Work

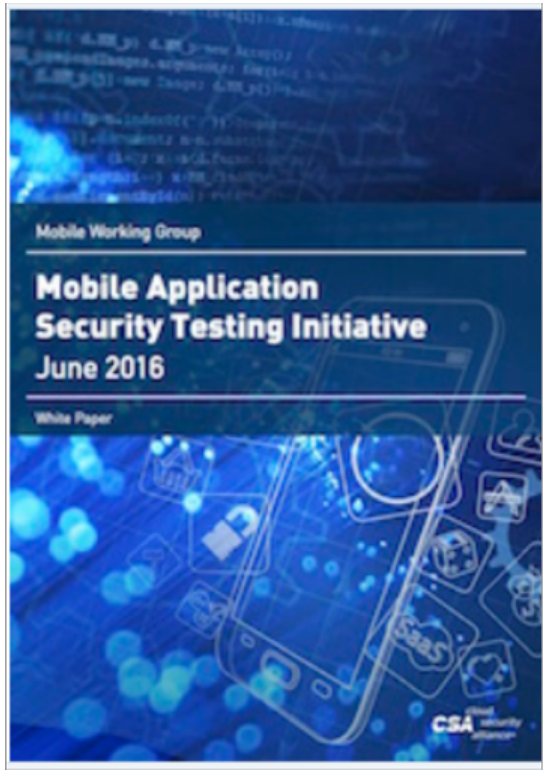
- Develop a mobile certification framework based on MAST control requirements & application vetting process

- Certified mobile apps can be issued a ‘MAST Trust Mark’ that gives users assurance that robust security testing has been undertaken

Join the MAST WG!

Companies Represented in WG

- OWASP
- ERCOT
- LGMS
- Standard Chartered
- Chevron
- University of Auckland
- UL
- Eforce Tech
- UTC
- CEPREI
- CISCO
- CSA Group
- CAT
- KPMG



Mobile Working Group

Mobile Application Security Testing Initiative June 2016

White Paper

Download our 2016 MAST whitepaper: http://bit.ly/2keCHa2

To join the WG, write to us at:

csa-apac-research@cloudsecurityalliance.org

Contact Us

General inquiries:

csa-apac-info@cloudsecurityalliance.org

Research information:

csa-apac-research@cloudsecurityalliance.org

Facebook: csaapac1

Twitter: @cloudsa_apac

LinkedIn: Cloud Security Alliance

Thank you