Mobile App Threat Monitoring

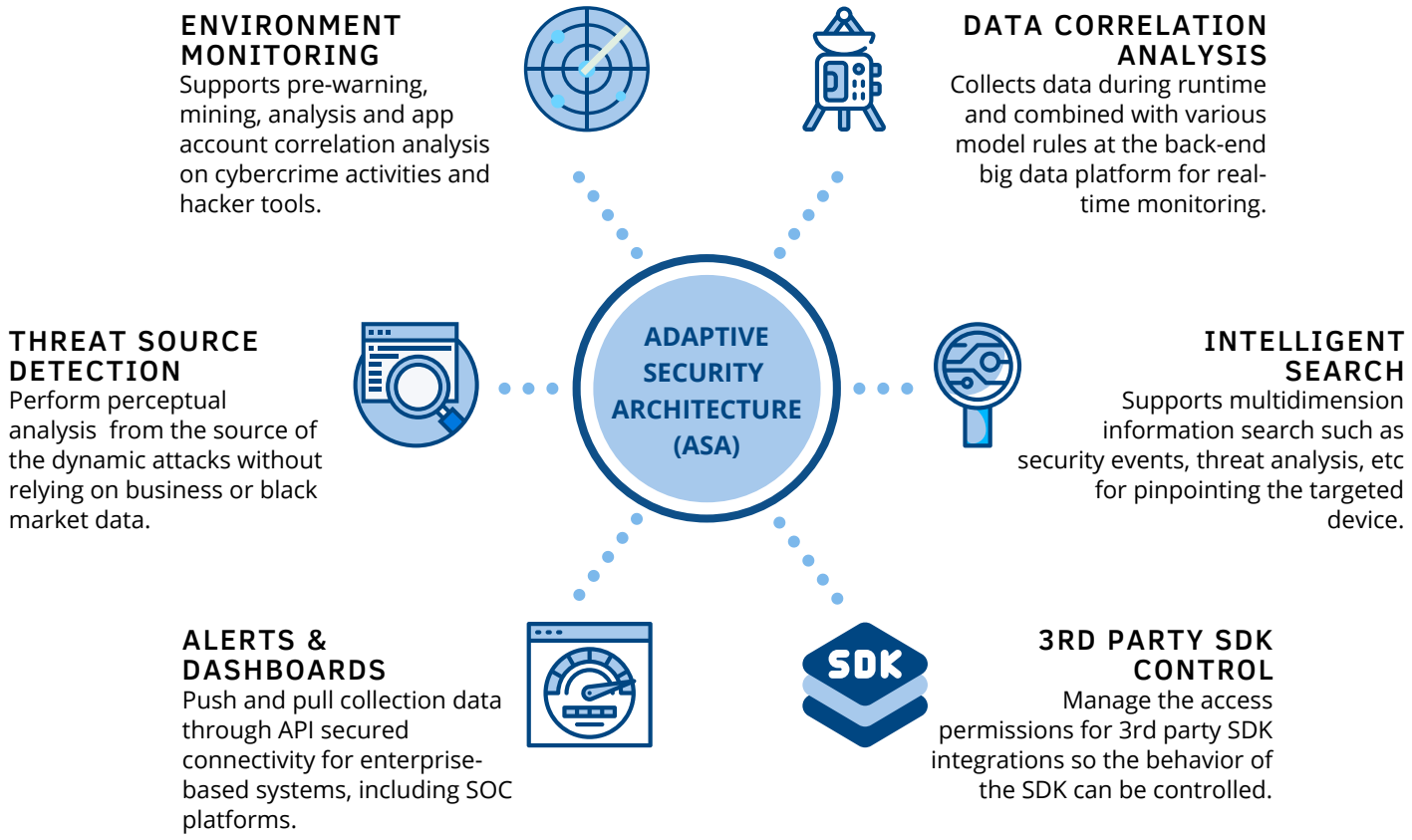
IRONSKY

MONITOR, MANAGE AND MOBILIZE YOUR DIGITAL FOOTPRINTS AGAINST POSSIBLE THREAT ATTACKS AT THE DEVICE AND APPLICATION LEVELS.

Highlights

TAILORED RECONNAISSANCE	RASP RUNTIME PROTECTION	AUTOMATIC RISK MANAGEMENT	REAL-TIME SECURITY
Investigative analytics of correlated data to pinpoint anomalies detected by incoming attackers.	Prevent runtime exploits on your applications by leveraging on a centralized security monitoring toolset.	Protect assets automatically from known and unknown mobile threats with unmatched detection and real-time responsive remediation.	Know exactly what's happening across your applications and users with real-time visibility on a dedicated dashboard.

Start protecting your digital assets beyond just your perimeter by extending your cyber defenses across applications, users and end devices. IronSKY Threat Monitoring eliminates risk by providing a daily assessment of your exposed assets' risks. It delivers this service through a unique combination of advanced technology and the world's leading threat intelligence. Stay up to date on the latest security and compliance trends and regulations. Get continuous visibility and insights into your enterprise so you can be confident that your mobile applications are safe, secure and compliant at all times. Deter the next threat before it impacts you or your business by learning from your risk mitigation efforts.



business@seciron.com www.seciron.com

All Rights Reserved 2021

IronSKY solution provides out-of-the-box, real-time monitoring of your organizations external and internal applications, giving security teams a single view of their entire security posture.

CORE SENSING FEATURES

Runtime Abnormality Detection & Analysis

EMULATOR
Protect your business-critical applications against emulators and simulation attacks. If you are not using a technology-enabled solution for detecting the presence of emulators, attackers can use them to emulate your systems and evade detection.

LOCATION FRAUD
Detect threats originating from GPS location spoofing, beaconing, and other similar applications that use location as a medium of transmitting the data. In addition to receiving alerts, IronSKY logs GPS coordinates, duration, IP address, time, and date.

DOMAIN NAME FRAUD
Prevent possible phishing scams on your users via redirections to another site. This is a type of attack in which a company's brand reputation is being used to fool consumers into visiting malicious websites.

PROGRAM PLUG-IN
Program plug-ins that are not recognized may contain malicious codes The protection is based on the principle of checking the digital signature of the application against a known list of valid signatures.

APP TAMPERING
Prevent the possibilities of cybercriminals from creating a fake version of your business application through app tampering techniques such as code injection, reverse engineering and modification of your application's database. These methods can be used to make the application's data appear fake, and subsequently compromise it. This means that you do not have to worry about another developer copying your application and creating a fake version, thereby putting the business data at risk.

DEVICE REUSE
Protection works by putting a wrapper around your app to ensure that it's only running on the intended hardware device. This prevents cloning of hardware-based applications and protects paid and free applications alike against tampering and theft.

INJECTION ATTACK
Detect malicious code injections during application runtime utilizing machine learning algorithms and prevent applications against code modifications, data theft, corrupted programs or system files and passwords.

DEBUGGING
Detects the type of debugging tools used such as a debugger, traceview or even DDMS tools. System will warn the user about potential security issues in the application, before they are executed.

SYSTEM ACCELERATION
Detect if an attacker tries to accelerate system of the mobile application by increasing the number of requests. If the same request is received several times, the mobile application will detect the attack and the system will display a warning alert.

ABNORMAL CERTIFICATES
Our solutions protect against certificate abnormality on mobile apps by inspecting and monitoring the certificate chains installed on the mobile app as well as the root of trust. This way we can ensure that the certificates used by the app are valid, trusted and detects abnormal certificate usage such as rogue certificates and fraudulent usage of legitimately issued certificates. These findings will then be reported to the IronSKY security management platform.

business@seciron.com
www.seciron.com
All Rights Reserved 2021

Runtime Environment Risk & Crash Detection

SENSITIVE CONFIGURATIONS

Intelligent probes monitor your applications on end-devices against sensitive configurations such as "USB debugging mode enabled" or "Mock App Location enabled". If a sensitive configuration is detected, a report of this detection is sent to a data repository and displayed on the live dashboard, where additional analysis can be performed by a human analyst or a security management team.

FRAMEWORK SOFTWARE

Detect and analyze anomalous behavior and events related to your mobile application framework software, like: buffer overflow attempts, analysis of Xposed hooks or Frida injector function calls, etc.

3RD PARTY APPS & PROCESSES

A point system that ranges from 1-5 is assigned to each application in our database. This helps identify applications that may pose a threat, but also allows for manual review of applications before they are automatically blocked.

ROOT/JAILBREAK

Detect possible root or jailbreaking attacks, even if the attacker is using popular tools such as Magisk Hide, Pegasus, EventBot or Xposed, providing greater coverage for your business and users.

CLICKJACKING & HIJACKING

Interface hijacking or UI redress attack on mobile apps is a malicious act of gaining unauthorized access to sensitive information of the user on the mobile device. It is a silent attack that happens in background without user's consent or awareness. An attacker uses transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. The UI redress attack detection capabilities in IronSKY helps security teams detect potentially compromised user accounts and perform a UI redress attack audit to investigate the scope of the threat.

APP NO RESPONSE/HANG

Detects runtime crashes such as deadlock, CPU overload, memory leaks, memory dump, null pointer exception, fatal exceptions, etc. which are not visible in the log files. It also detects memory corruption, thread pools issues, and provides a visual indicator for each on the live dashboard. In addition, it captures various attributes of the application including its name, version, package path, JNI libraries, size, and class loaders.

APP PROCESS CRASH

Identifies application process crashes which are caused by potential exploits such as Uncaught exceptions, invalid pointer dereferences, native crashes and memory leaks. Our engine uses a variety of detection methods to look for signatures in process memory, and to query the running process' address space to determine possible execution paths.

SYSTEM SERVICE CRASH

Protect applications against possible system service crashes such as tombstone creation, file system event changes, and writes to the registry. Many of these anomalous events are likely indicative of attacks on user data or application system state. We are able to detect many of these events by monitoring application service requests that are associated with applications that are commonly targeted by attackers.

KERNEL CRITICAL ERROR

The platform identifies null pointers, memory leaks, use-after-free, buffer overflows, the use of strcpy, sprintf, or other vulnerable string copy functions that can lead to system crashes. This vulnerability may be exploited remotely to take control of an affected device. IronSKY framework notifies software developers of vulnerabilities in their applications as soon as they are detected. By identifying and notifying application developers about these problems quickly allows for the most effective response and prevention method against potential security breaches and loss of sensitive data.

business@seciron.com

www.seciron.com

All Rights Reserved 2021

ATTRIBUTES	FEATURE HIGHLIGHTS	BENEFITS
Live-Dashboard	- Enterprise ready - Real-time attack information - Global threat monitoring with statistics, timelines, and classifications.	Easily monitor and analyse potential incoming threats from occurring on applications and devices.
Easy Deployment	- On-premises - SaaS (Cloud) - Private (Cloud) - API Push & Pull data	Choose the best method to secure that suite your organizations requirements.
Simple SDK Integration	- Easy probe SDK integration - Works in the background without disrupting UX functionality	Maintain SDK application performance without any disruptions.
Threat Detection Capabilities	Runtime Environment Detection - Jailbreak - Root detection - Framework software - Risk application - Risk process - Sensitive configuration - Interface hijacking Runtime Abnormal Behaviour Detection - Crash monitoring - Https hijacking - Application crack - Emulator - Device reuse - Location fraud - Domain name fraud - Injection attack - Debugging behaviour - System acceleration - Program plug-in - Abnormal activity - Change frequency of IP, device, location, account ID	IronSKY offers a more comprehensive overview of security threats. This assists organisations and businesses in Improving visibility and awareness into mobile software applications from vulnerabilities and threats.
SDK Access Controls Capabilities	Permissions of different SDKs are customized on the server-side to achieve limitation of sensitive data collection. - SMS - Device information - Phone number - Address book - Location information - Application installation list - Photo / video - WIFI - Bluetooth	By setting policies, it can prevent certain SDKs from exhibiting unauthorized behaviour by blocking the SDK's requests for permission. This improves the security of the overall system by reducing the risk posed by individual apps.
Real-Time Threat Response Notifications	Admin selects the threats for which they want a notification sent to the security teams once a threat is detected on the applications and devices. Messages can be customized and created in multiple languages.	Configurable alerts and notifications of threats detected on application and device.
Automated Runtime Threat Response	Create security action configurations and policies based on device and threat type. Admin selects process flow for each enumerated. - Silent Monitoring - Alert - Alert with optional exit - Alert with force exit - Blacklist	With or without Internet connectivity, security protocol actions and threat notifications are continuously performed. The mobile device becomes the first line of defence against threats and attacks and can significantly shorten the “kill chain” for attacks originating from the mobile device.

All Rights Reserved 2021

Evolving Security Requirements

IronSKY Mobile Threat Monitoring provides an early warning across your entire digital perimeter against evolving threats, enabling you to detect and prevent new attacks while minimizing disruptions to your critical IT environment.

Invisible to the naked eye, vulnerabilities and problems can lurk in the deep web. We provide insight into the digital threats that could affect your organization and provide a checklist of things to take away from the threat landscape. We help you to identify vulnerabilities and protect against them, while providing a full view of your data, providing your organization with total benefits that increases the value of your business:

- **RELEVANCE**

  Mobile App Threat Monitoring specifically tailored to your organizations needs and requirements.

- **READINESS**

  Wide range of detection items and capabilities. Flexible policy arrangements to cater for different scenarios.

- **RELIABILITY**

  Identify the real threat to your environment and minimize false-positive detection.

- **COMPATIBILITY**

  Real-Time Threat Monitoring is available for Android, iOS, native, hybrid, and cross platform apps. For HarmonyOS, please enquire with your dedicated account manager.

- **VISIBILITY**

  Live monitoring interface provides 24/7 overview of your entire security posture and incoming attacks so you never miss a possible threat.

- **EXPERTISE**

  Industry leading security experts with over a decade in dedicated experience, and the latest studies and updates on global threats from current to potential future exposures.

Total Support

We provide unsurmountable dedication to supporting our customers 24/7 across regions for any troubleshoot or technical assistance. Consult your account managers for additional support assistance when required.

Privacy & Sensitive Data Security

A properly configured RASP security and lockdown policy, coupled with IronWALL application hardening, gives a multi-layer security platform protecting your data assets and end-users privately identifying information. This ensures a high level of protection, while giving the flexibility and functionality that users require from today's end-user devices.

SECIRON

Over A Decade of Providing Security Solutions Across Asia

We are the industry leader in mobile application security across Asia. With over 10,000 applications across 9 countries protected using our End-to-End solutions, industries across Banking, FinTech, Insurance, Gaming & Government choose us to secure their applications across end-devices.

Connect with us to know more

Get In Touch
business@seciron.com
www.seciron.com

SecIron reserves the right to make changes to specifications at any time and without notice. The information furnished in this document is believed to be accurate and reliable. However, SecIron may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use. Last Update September 2021.

All Rights Reserved 2021