Intellyx™

Integrating Mobile Threat Alerts for Total Risk Visibility

An Intellyx Whitepaper for Verimatrix
by Eric Newcomer, CTO and Principal Analyst

Fall 2025

Introduction

Organizations reduce mobile app risk by controlling applications employees use for business purposes such as corporate email, conference calls, phone calls, text, and document sharing.

In addition, many organizations offer mobile apps for their customers. It's at the point now where it's a competitive issue – every business offers a mobile application to its customers as part of the customer experience, and to increase revenues and "stickiness."

With businesses so focused on mobile applications, the growing use of mobile devices by an increasingly mobile (and remote) workforce, and the proliferation of customer focused mobile apps, how does an organization bring it all together and get a comprehensive view of their overall security risks and vulnerabilities?

Many organizations already have a Security Operations Center (SOC) to monitor security vulnerabilities, risks, and alerts across the organization's internal network.

Mobile devices, however, run outside the organization's network perimeter and are not directly under the control of the cybersecurity staff, opening up a new set of risks and vulnerabilities.

Mobile applications, for example, typically communicate back into the IT environment using public APIs.

If someone breaks into an organization's mobile app or steals someone's login information (via phishing social engineering, or brute force) not only is the information in that app at risk, but also the data and systems on the server side that can be reached through those APIs.

Mobile apps are vulnerable to wiretapping, man in the middle attacks, data theft, malicious app installations, malware, code tampering, reverse engineering, and control failures to name but a few threats.

An organization needs to not only protect its mobile applications with a solid security solution with threat monitoring and alerting, but also ensure it protects against break ins on the server side as well.

That protection includes integrating mobile app security alerts into the organization's SOC.

The Security Operations Center (SOC)

The Security Operations Center (SOC) is the place where security analysts check for alerts – especially red alerts – and respond to and remediate incidents and breaches as quickly as possible.

A traditional SOC monitors the corporate network, applications on the corporate network, and applications deployed in an organization's public cloud accounts.

So a traditional SOC, which is designed to monitor the organization's network, and to receive alerts from applications and network devices, is not typically designed for monitoring mobile networks or mobile applications.

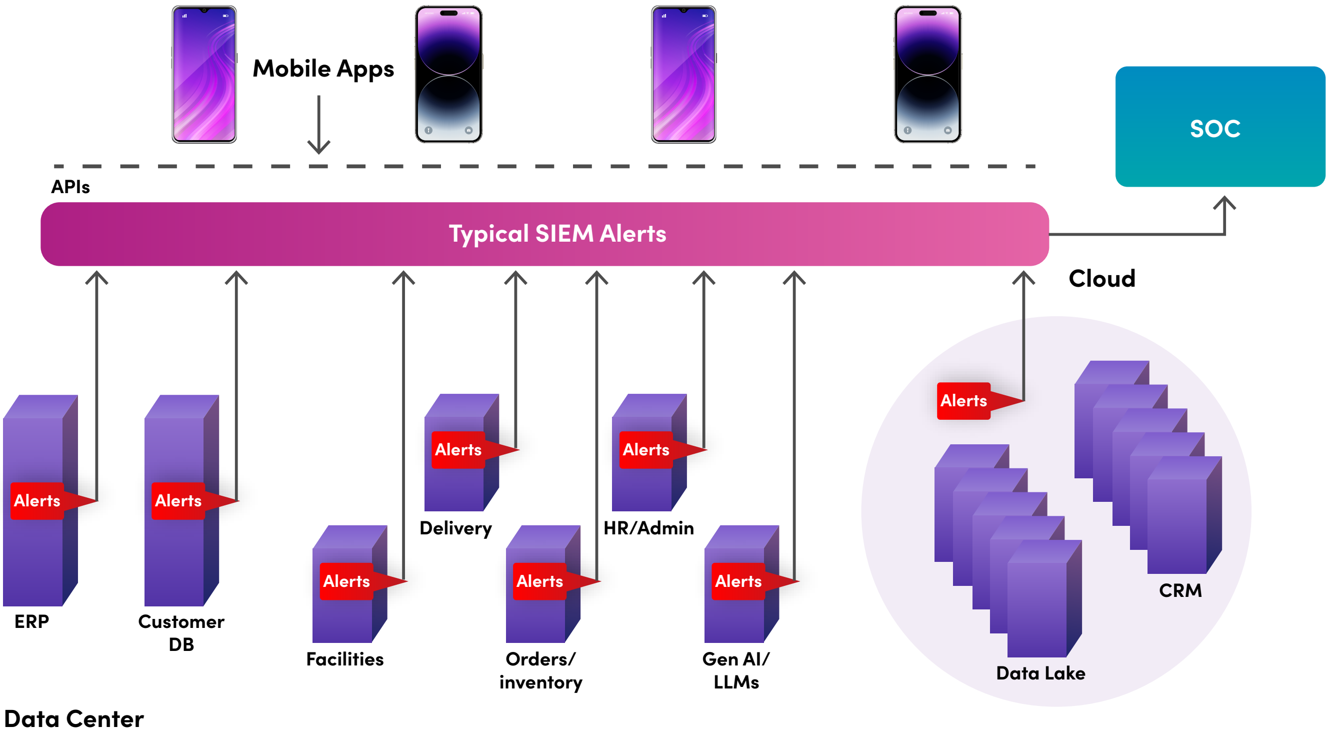

Figure 1: A SIEM Solution That Does Not Capture Mobile Threat Alerts
Figure 1 depicts applications of an organization with a typical SIEM solution feeding security events and risk alerts from internal network and cloud account-based applications to the SOC.

The illustration also depicts mobile applications that are running outside the corporate network, but which call into the network using public APIs. Mobile applications and their APIs not only need to be protected, alerts from them also need to be integrated with the SIEM solution for complete SOC coverage.

In other words, a traditional SOC must be updated with a way to include threat alerts from applications outside the traditional enterprise and cloud account networks.

The best way to do that is to pass mobile application threat alerts to the SOC using a SIEM (security information and event management) solution. Most organizations with a SOC already have a SIEM solution in place.

SIEM systems extended to include mobile applications provide a complete picture to the SOC of all an organization's vulnerabilities and threats, whether from the internal network, cloud account, or mobile applications.

A SOC typically operates around the clock so that if a cyberattack is detected, such as a DDOS or a credential stuffing attack on an API, someone notices and takes action to block the attack and remediate the risk.

Responses to cyber-attacks typically follow playbooks that identify responsible parties, such as application owners, network operations, database administrators, and production support staff working in the area where a breach is discovered. The responsible parties diagnose the issue and fix it.

For a DDOS attack, for example, this is typically the team responsible for operating and supporting the organization's web application firewall (WAF), which is configured to prevent a DDOS. When a DDOS attacker finds a way to defeat existing defenses, the SIEM system fires an alert to the SOC and the SOC contacts the WAF support team to diagnose and fix the issue.

For an API attack, the SOC team typically contacts the development team responsible for maintaining the API and the team responsible for API security. In some cases, additional teams may be included who are responsible for preventing and addressing credential stuffing attacks.

In any case, the SOC team will need information collected from the mobile applications to diagnose the issue, select the right playbook, and identify the right team (or teams) to contact to fix the issue.

Successful integration of mobile application alerts to the SIEM solution therefore requires coordination with the SOC team as well, not just the capability to send alerts.

A playbook or response process, along with the teams responsible for the mobile apps, must be included. As the old maxim says, SOC integration requires coordination across technology, people, and processes.

Passing Mobile Threat Alerts in SIEM Data

The mobile applications your employees and customers use need to be integrated with the SOC monitoring systems you're already using to protect your applications and public APIs from attacks that exploit vulnerabilities on the mobile device.

Phishing and social engineering attacks are among the biggest causes of mobile device incidents and breaches, along with brute force stolen credentials.

First you need a mobile app protection solution that will also protect your network and APIs.

This mobile app protection solution should include integrating with a SIEM solution such as Splunk or LogRythm, IBM Qradar, or ArcSight to notify the SOC of any security alerts or risks.

The best approach is to first identify the data model the SOC is using to ingest data and then send mobile device alerts in that format.

If it's Splunk, for example, use the Splunk Common Information Model (CIM).

The app security solution on the mobile device should be capable of producing and sending the type of alerts the SOC expects to see, such as Verimatrix XTD's API does.

The XTD API provides a direct way to ingest analytics information as a stream, getting access to all the relevant data in near real-time.

In addition, the XTD API provides basic filtering of events to narrow the scope of the retrieved information as necessary.

Polling the API is required if you need continuous access to the analytics, however. So it's important to decide how often and how frequently to poll the API to access the mobile data, for example whether you need real time analytics for active monitoring or a daily feed for reporting purposes.

The API returns data in either JSON or CSV format, including the following items:

- A unique ID string for filtering duplicates
- The risk level of the alert (low/suspicious/high)
- A customer assigned application ID
- The type of risk detected and when it was detected
- The application package ID
- A UUID to identify the application instance
- The operating system and version (Android, iOS, or iPadOS)
- A geo location indicator
- The masked IP address of the remote application instance
- A pagination cursor control to poll data over time.

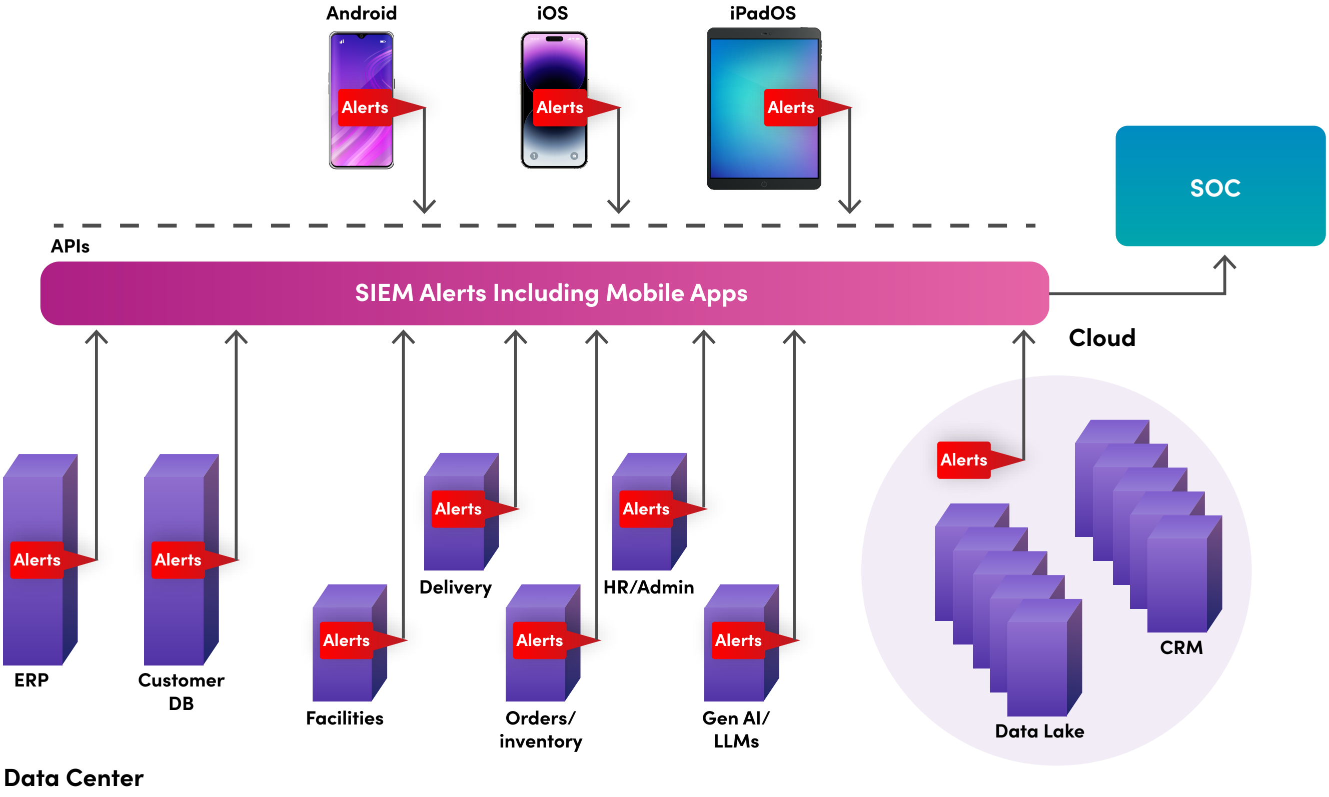

Figure 2: A SIEM Solution Including Mobile Threat Alerts

The result looks like Figure 2, with the mobile devices now integrated into the SIEM system an organization is already using for feeding data center and cloud alerts to the SOC.

Verimatrix provides the means to pull the data from its XTD SIEM API but does not integrate directly into any specific SIEM vendor system.

To use the data retrieved by the Verimatrix SIEM API, you have to configure and/or write a custom data processing module. This could be a simple HTTP retriever plugin or a custom, daemon-like process that pulls the data and then performs a push to the SIEM you're using.

In other words, you have to write or configure some code to call the XTD API to retrieve the data from the mobile app log, reformat it for your SIEM solution's data model, and push it to the SIEM solution.

The XTD SIEM API provides a 24 hour, rolling window view of the available log data. At any given point, a request to the XTD API has at most 24 hours of data available. A data request must consider the rolling window, and the fact that data at the back of that window is no longer available after 24 hours.

If a continuous set of data is required, the API caller must ensure that data is polled at regular intervals.

Verimatrix XTD API Solution

The Verimatrix XTD API extracts data kept within the mobile app that tracks security issues. XTD publishes an OpenAPI spec that defines the API for ease of adoption.

The XTD API accesses the risk data from the mobile application so you can feed it to a SIEM solution, which passes it to the SOC along with other security alert and monitoring data from the rest of the enterprise.

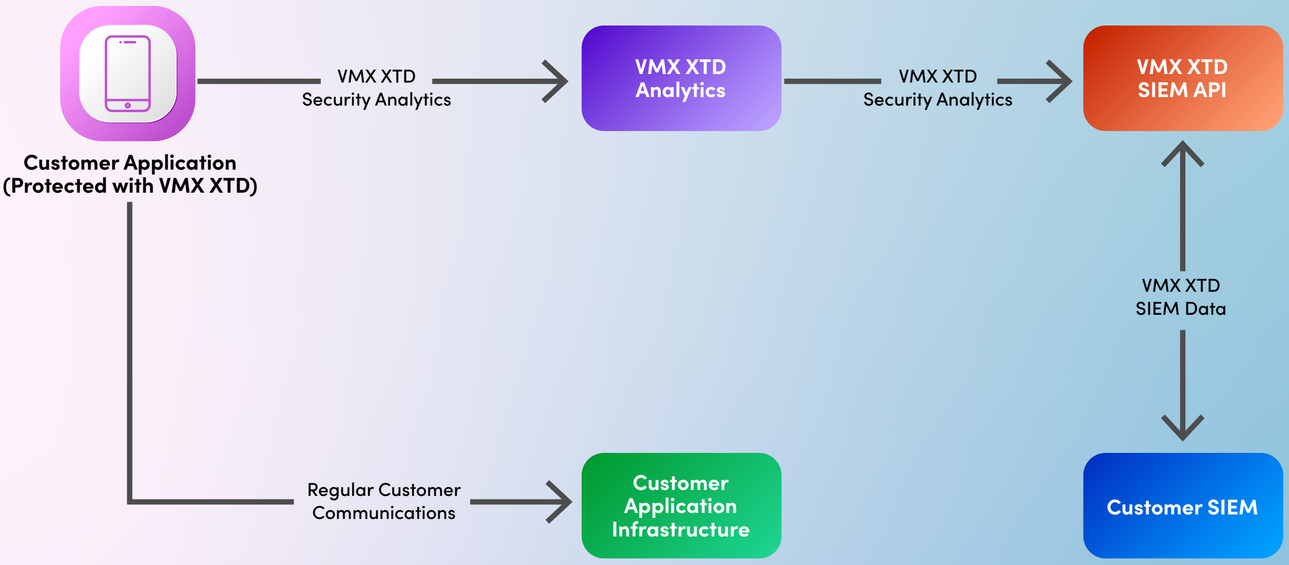

Figure 3: Verimatrix XTD API for Retrieving Threat Alerts
This diagram in Figure 3 illustrates a mobile application protected using Verimatrix XTD, which provides an API channel for retrieving security analytics information.

The primary communications channel is to the backend server infrastructure supporting the mobile application for its normal business function, whether for shopping, banking, travel booking, health care, etc.

The primary communication channel is what XTD is designed to protect. XTD protects the mobile application from risks and vulnerabilities, and in doing so produces analytics that are stored along with the application.

XTD supports a second communication channel for retrieving the security analytics and forwarding them to an organization's SIEM technology, such as Splunk, LogRythm, or ArcSight.

The XTD API requires authentication using the Verimatrix platform API keys, which can be generated using the Verimatrix portal. An API key is exchanged for a short-lived access token, which in turn is used when calling the API.

Basic requests use an HTTP GET with a header specifying the response format. A request can put a limit on the number of replies, filter by risk level, and access data within a given date and time range.

API users determine the frequency of access to mobile alerts. The data is available for a 24-hour time window, and users of the API determine how often they want to retrieve the data and push it to the SOC.

The Intellyx Take

Security risks and alerts are not always of equal priority or consequence, but it can only take a single incident to cause significant damage, both financial and reputational.

And it's always the unlocked door, the keys in the ignition, the wallet or phone left out in the open that cause the most problems.

In other words, leave no stone unturned in the fight against cybercrime. Mobile apps may not be part of the organization's network, but they have credentials, data, and APIs that access sensitive server-side information.

Protecting mobile applications becomes more of a priority and more of a risk every day as mobile applications grow more popular, and are increasingly used for business, ecommerce, banking, and health care, to name a few.

Putting mobile application risks into the right context with other cybersecurity risks should be a priority for any organization that wants to sleep well at night. Mobile app security holes should be filled, including consolidating alerts for organizational SIEM solutions.

Verimatrix XTD offers a comprehensive mobile application security solution that protects apps and gathers analytics, including security alerts.

The analytics data is available via the XTD API for a period of 24 hours and can be consumed and forwarded to the SOC at intervals that make the most sense for the organization's security strategy.

Alerts sent to the SOC team helps them take immediate and appropriate action before it's too late.

About the Author

Eric Newcomer is CTO and Principal Analyst at Intellyx, a technology analysis firm focused on enterprise digital transformation and AI transformation.

Eric was CTO of WSO2 before joining Intellyx in 2023 and was CTO of IONA Technologies until its acquisition by Progress Software in 2008.

Eric is an internationally recognized expert in transaction processing, web services, SOA, and cloud migration. His books on transaction processing, web services, and SOA have been translated into multiple languages and are used as textbooks in universities across the globe.

In financial services Eric served as Global Head of Security Architecture at Citi's Consumer Bank, Chief Architect at Citi's Treasury and Trade Services Division, and Chief Architect at Credit Suisse's Investment Banking Division.

Eric started his career in technology at Digital Equipment Corporation (now part of HP), where he was elected Distinguished Engineer as a Transaction Processing Architect.

verimatrix

DRIVING TRUST

About Verimatrix

Verimatrix (Euronext Paris: VMX, FR0010291245) secures the apps that power our digital world. The Verimatrix Extended Threat Defense platform (XTD) delivers next-generation app protection for Android, iOS, embedded, and desktop apps—blending layered shielding, adaptive AI-driven threat intelligence, real-time detection and response, and whitebox cryptography to block attacks before they happen. Built for modern development, XTD integrates seamlessly with CI/CD pipelines and SIEMs—boosting security without slowing innovation. For 30 years, global leaders have relied on us to build trusted, seamless digital experiences—without compromise. Backed by ISO-certified security, 150+ patents, and award-winning localized services in 9 countries, we protect industries like telecom, hospitality, banking, e-commerce, healthcare, and automotive from relentless cyber threats. The apps we trust need protection. Verimatrix delivers.

Visit **www.verimatrix.com/cybersecurity**