



SKYFORMATION for HOME-GROWN APPS

Govern home-grown applications security and compliance risks

Overview

Business applications (aka Home-grown applications) developed by the organizations provide a broad set of business processes and service functions.

Home-grown applications are built for mobility and data collaboration. These applications are delivered on public, private, hybrid or traditional infrastructure.

Organizations developing home-grown applications are responsible for security aspects, such as:

- DETECT and REMEDIATE THREATS
- ENSURE SECURE CONFIGURATION
- ACCEPTABLE ATTACK SURFACE
- RETAIN FULL SECURITY AUDIT TRAIL
- KEEP REGULATION COMPLIANCE

What will SkyFormation for Home-grown Apps do?

PROVIDE SDK for HOME-GROWN APPS DEVELOPMENT TEAMS

SkyFormation provides development teams with SDK that allows simplest way for them to log security events in a unified form with the data needed.



MONITOR SECURITY EVENTS ACROSS HOME-GROWN APPS

Using its unique technology, SkyFormation collects and enrich the Home-grown apps security events created using its SDK. The events are then sent in an actionable form to enriched with the required business content and sent to the SkyFormation platform for additional analysis and detection.



Solution Highlights

SkyFormation for Home-grown Applications allow organizations to:

- Extend their SoC SIEM/Splunk to cover private business applications.
- Detect insider and external threats
- Streamline Investigation of security incidents
- Speed up regulatory compliance support

EXTEND THE ORGANIZATION SIEM/SPLUNK to COVER HOME-GROWN APPS

SkyFormation integrates with the organization's SIEM/Splunk and sends the entire security events and alerts identified by the SkyFormation connectors. The organization SIEM/Splunk retrieves the events in an actionable correlation ready state. SkyFormation unified security events language ensures that correlations could be done once and applied across multiple applications.

EXTEND THE ORGANIZATION REMEDIATION TOOLS to COVER HOME-GROWN APPS

SkyFormation provides an open API for remediation actions, such as "disable user", "remove file" and more across its home-grown connectors. This allows the organization's existing remediation and incident response tools to integrate and execute remediation actions on the home-grown applications and eliminate their need in writing dedicated connectors.

EXTEND THE ORGANIZATION CENTRAL LOG with HOME-GROWN APPS SECURITY AUDIT TRAIL

SkyFormation platform can be configured to send the entire collected unified security events from any home-grown application into the organization's central log server. This would streamline the SoC investigation process, and ensure full audit trail for compliance or forensic according to the organization's needs.



"SkyFormation allows us to detect threaten activities on our core cloud applications using our existing best of breed SIEM/SoC tools and expertise. So simple and so effective"
Ron Gal, Chief Information Security Officer at NICE technologies

Why use SkyFormation for Home-grown apps?

- **ONE SECURITY SUITE for ANY TYPE OF APPLICATION**

SkyFormation for home-grown apps ensure that the same security detection, investigation and remediation cover any type of applications. The best security coverage at the lowest costs.

- **NON-INTRUSIVE (out-of-band)**

SkyFormation uses only out-of-band technologies for its monitoring and other needs. It does not need proxy; therefore, imposes zero risk to the organization's security or the cloud applications availability.

- **DEPLOYED ON-PREMISE**

SkyFormation platform is a software-only solution, which can be installed on any Windows or Linux platform deployed either on-premise or in the organization's cloud infrastructure. Therefore, the organization's sensitive security activities, cloud applications credentials and shadow-IT analysis information gathered by SkyFormation stays within its domain.

About SkyFormation

Founded in 2014, SkyFormation is a new type of cloud access security broker (CASB) platform. It provides both cloud and home-grown applications (e.g. Google Apps, Salesforce, Office 365, Private app) with a single point of security visibility and threats protection, by extending the organization's existing Security Operations Center (SoC) tools as SIEM/Splunk to cover cloud applications.