VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

WOMEN OWNED

GRC
Datasheet

VANGUARD ACTIVE ALERTS

Monitor all of your organization's CA ACF2™, CA Top Secret® or IBM RACF®. security events.

PRODUCT DESCRIPTION

Vanguard Active Alerts for RACF, ACF2, and Top Secret (TSS) is a z/OS™ started task that continuously filters System Management Facility (SMF) events looking for system and user-specified types of events. When one of these types of events are found, Vanguard Active Alerts will send a user-defined notification for the type of event that has occurred.

BUSINESS CHALLENGE

Mainframes share a lot of information about what’s happening (event log, audit log, syslog, etc.), Organizations need to achieve a way to quickly and easily separate critical security incidents from business-as-usual events and send them in the right format to your enterprise.

VANGUARD SOLUTION

Vanguard Active Alerts provide the ability to continuously monitor security related events at the system and/or user-specified level. When an event occurs, Vanguard Active Alerts will notify the SIEM (Security Information and Event Management) in order for enterprises to take decisive action and make critical business decisions.

KEY FEATURES

- Delivers mainframe data to all conventional SIEM products
- Connects with standard z/OS security products
- Monitors z/OS and UNIX System Services (USS)
- Gathers intelligence from z/OS SMF
- Provides customized real-time alerts that can be managed, filtered, routed, and searched via SIEM
- Allows APIs for defining and filtering TSO, CICS, and batch events

KEY BENEFITS

- Real-time monitoring
- Flexible with all SIEM providers
- Adheres to compliance & audit requirements
- Installs easily and doesn't require z/OS IPLs
- Uses a small footprint in each LPAR, with little CPU overhead

SCAN THE QR CODE TO LEARN MORE

GRC
Datasheet

VANGUARD ACTIVE ALERTS

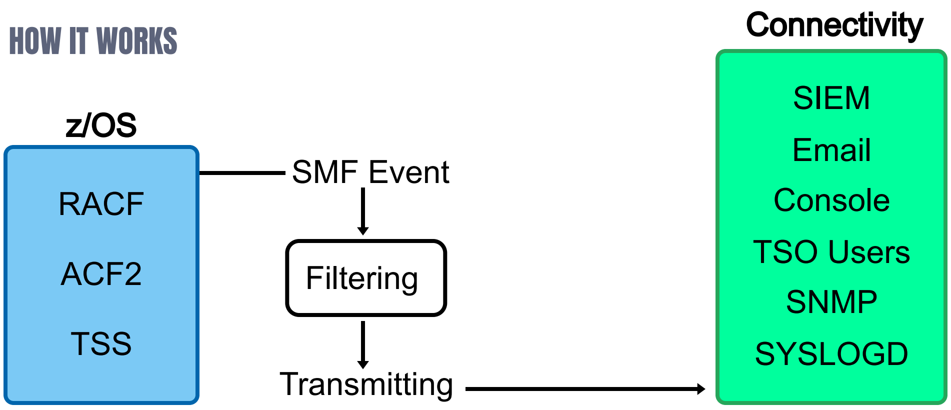
PRODUCT DETAILS

Vanguard Active Alerts sends user-specified event driven data to SIEMs, SNMP or SYSLOGD in industry-standard formats as requested by the user. Active Alerts send event-driven data to identified target devices, which receives the real-time information in a timely manner for compliance, security and audit requirements.

Modes of notification include:

- Email
- Console
- Security Information and Event Management (SIEM) notification
- Simple Network Management Protocol (SNMP)
- TSO Users
- SYSLOGD

HOW IT WORKS



VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS WOMEN OWNED®

GRC
Datasheet

VANGUARD ACTIVE ALERTS FOR SIEM

PRODUCT DESCRIPTION

SIEM (Security Information and Event Management) software such as Splunk® is a comprehensive security solution that collects, analyzes, and manages security event logs and data to enable real-time threat detection, incident response, and compliance management.

Vanguard Active Alerts for Splunk is a web-styled dashboard interface that displays events retrieved via Vanguard Active Alerts from SMF records on these External Security Managers (ESM): CA ACF2™, CA Top Secret® (TSS), and IBM RACF® systems. With this product, you will be able to monitor, search, analyze and visualize active alert data in real-time. Vanguard Active Alerts for Splunk can capture, index and correlate your data and then present it in graphs and alerts on various dashboards.

HOW ACTIVE ALERTS WORK IN THE SPLUNK SIEM ECOSYSTEM

Event Detection Types

Vanguard Active Alerts for Splunk detects access violations, invalid users, and expired passwords within a specified time period.

Event Types

Vanguard Active Alerts for Splunk has the following event types covering RACF, ACF2 and Top Secret.
(NOTE: the example below are only partial lists of all the event types)

RACF

- Access Violations
- Assignment of SPECIAL, OPERATIONS, or AUDITOR user privileges
- Assignment of a Group Attribute or Authority
- Data Set Profile Universal Access set to greater than NONE
- Data Set Profile Universal Access set to greater than READ
- Access Granted due to Profile in WARNING Mode
- Invalid and expired Passwords within a Specified Time Period
- Password Recycling

ACF2

- Access Violations (Data Set and Resource)
- Assignment of ACCOUNT, LEADER or SECURITY user privileges
- Assignment of WRITE(A), SERVICE(UPDATE) or $MODE(QUIET) to UID(*)
- Assignment of READ(A), ALLOCATE(L) or SERVICE(READ) to UID(*)
- Access Granted due to a Data Set Rule in WARNING Mode
- SMF Lost Data Detection
- PDS or PDSE member activity (add, delete, replace and rename)

Top Secret (TSS)

- Access Violations (Data Set and Resource)
- Assignment of NODSNCHK, NORESCHK or NOPWCHG ACID privileges
- Assignment of authorities SUSPEND, CERTAUTH, MLSADMIN or PWMAINT to an ACID
- Control Options ADSP(YES), BACKUP(OFF), DEBUG(ON) or LOG(NONE) are set via commands
- SMF Lost Data Detection
- PDS or PDSE member activity (add, delete, replace and rename)

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS WOMEN OWNED®

GRC

Datasheet

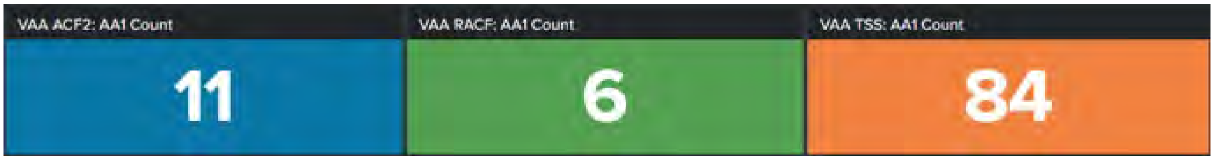
VANGUARD ACTIVE ALERTS FOR SIEM

SPLUNK® DASHBOARDS

Dashboards are an interactive web-based interface containing search boxes, fields and data visualizations. Each of the Active Alerts have their own unified dashboard displaying the following features and options:

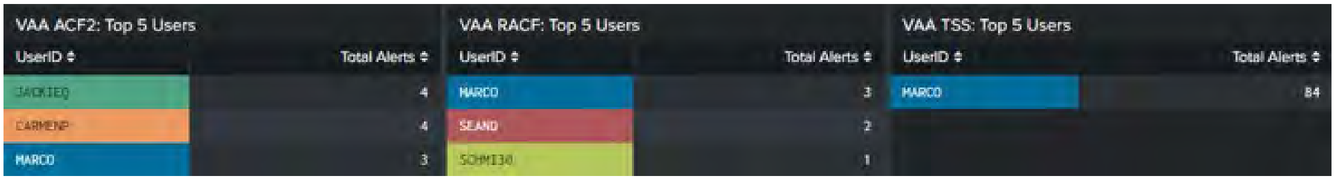
- Time Picker
- Change ESM
- Total # of Active Alerts
- Filters
- Time Chart
- Total Count of Different Access Levels
- Top 5 Users Triggering Active Alerts
- Breakdown Table

This section of the dashboard displays the total number of results side-by-side for CA ACF2™, IBM RACF® and CA Top Secret®.



VAA ACF2: AA1 Count	VAA RACF: AA1 Count	VAA TSS: AA1 Count
11	6	84

This section of the dashboard displays a table which lists the top five users who triggered the alert along with how many alerts were triggered. These results are displayed side-by-side for ACF2, RACF and Top Secret.



VAA ACF2: Top 5 Users

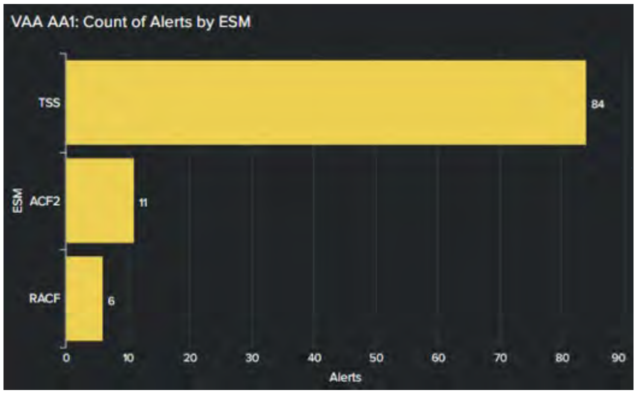
UserID ⇕	Total Alerts ⇕
JACKIEQ	4
CARMENP	4
MARCO	3

VAA RACF: Top 5 Users

UserID ⇕	Total Alerts ⇕
MARCO	3
SEAND	2
SCHMI30	1

VAA TSS: Top 5 Users

UserID ⇕	Total Alerts ⇕
MARCO	84



COMBINATION DASHBOARDS

The Combination Dashboards display the combined active alert data for the following ESMs: RACF, ACF2 and Top Secret covering the alerts that the ESMs have in common.

This Combination Dashboard example displays a horizontal chart for each ESM associated with the alert.

Note: If your organization is using all three of these ESMs, then the dashboard compares all three; however, if your company is using just two ESMs, then only two would appear.