Centrify
ZERO TRUST PRIVILEGE

splunk>

Centrify Zero Trust Privilege for Splunk

Seamless SIEM integration to thwart in-progress attacks

Data breaches are constantly on the rise — according to a recent Verizon report, 70% of breaches involving insider misuse took months or years to recover from the damage. Identity-related attacks are becoming more sophisticated and target environments with too many shared accounts and admins with too much privilege. To protect against these types of attacks, organizations need visibility across the privileged access activity in their environment to identify risk and act against attacks already in progress.

The Need for a Centralized View

High-profile breaches, insider threats and numerous regulatory and industry security standards are highlighting the risks associated with poorly managed privileged access to corporate systems. In many organizations, administrators are routinely granted broad privileges to accomplish narrow tasks. Malicious users, bots and malware are relentless in their pursuit of this type of broad access and the anonymity that shared accounts represent, and many of these bad actors go unnoticed as they navigate the organization.

Security information and event management (SIEM) technology supports threat detection and security incident response through real-time and historical analysis of security events from a wide variety of event and contextual data sources. The core capabilities of SIEM technology are a broad scope of event collections and the ability to correlate and analyze events across disparate sources.

Privileged Access Management Meets SIEM

One of the guiding principles of privileged access management is to implement least privilege access to reduce the attack surface. Least privilege access provides strong controls over user's privilege and reduces the risk associated with shared accounts and too much privilege.

With Centrify, users log in as themselves for their daily tasks, elevating privilege when necessary. Centrify's patented Zones Technology provides highly granular, role-based access controls that simplify the implementation of a least privilege access model.

The combined benefits of Centrify Zero Trust Privilege solutions and Splunk's SIEM solutions enable security teams to quickly detect and respond to internal and external attacks, simplify threat management while minimizing risk and safeguard organizations.

Leveraging SIEM Without Additional Costs

Centrify Zero Trust Privilege Services leverage a customer's existing investment in Active Directory to provide centralized identity management and monitoring across Windows, Linux and UNIX servers both on premises and in the cloud. Centrify Zero Trust Privilege Services integrate with Splunk's SIEM tools to provide privileged access data attributed to the individual user. This enables real time analysis to identify potential attacks already in progress.

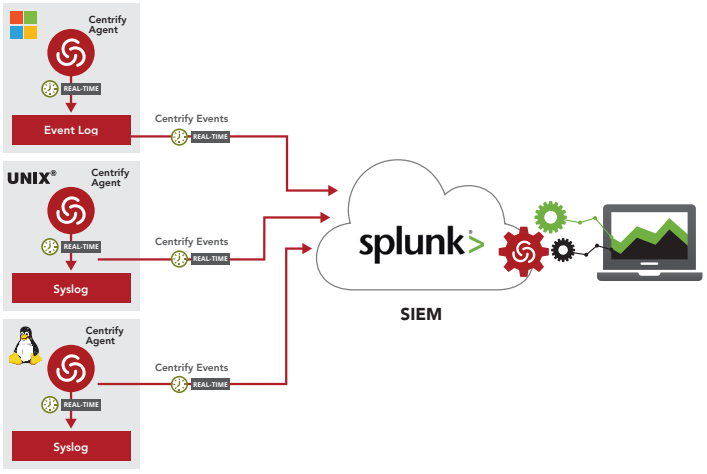
Easily Import Categorized Privileged Access Data

Centrify Zero Trust Privilege Services capture privileged activity associated with an individual and normalizes the data for consumption by Splunk's SIEM solution. These, and other infrastructure system events are correlated for centralized alert creation to identify the most critical security issues across the organization and facilitate the interruption of an attack.

How It Works

Centrify's agent can track over 300 different types of events in real-time on 450+ flavors of Windows, Linux and UNIX machines. A few sample categories of the Centrify events are:

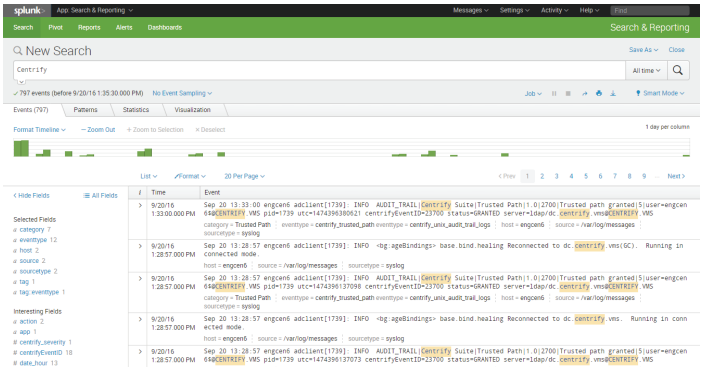
- User activity events on Centrify tools
- Log in events on Windows, Linux and UNIX systems
- Privilege escalation events on Windows, Linux and UNIX systems



Centrify events are available locally in standard logs either in Syslogs or Windows event logs.

Splunk's Common Information Model

Splunk's Common Information Model (CIM) enables the tagging of common events from a variety of vendors or source types, resulting in the unification of events from the data domain of interest across the enterprise. Centrify has mapped events to Splunk's authentication data model and can easily be found as shown in the following image.



Easily Searchable Events

Centrify event data is categorized and normalized prior to input into the Splunk database. The following is a list of all the Centrify event categories and their corresponding Splunk event type.

Centrify Event Category	Splunk Event Type
DirectAudit System Management	centrify_directaudit_system_management
Audit Manager	centrify_audit_manager
Audit Analyzer	centrify_audit_analyzer
DirectAuthorize - Windows	centrify_directauthorize_windows
DirectAudit ¬ Windows	centrify_directaudit_windows
Centrify Configuration	centrify_configuration
DirectControl UNIX Agent	centrify_directcontrol_unix_agent
DirectAudit UNIX Agent	centrify_directaudit_unix_agent
Centrify Commands	centrify_commands
Trusted Path	centrify_trusted_path
PAM	centrify_pam
dzdo	centrify_dzdo
dzsh	centrify_dzsh
dzinfo	centrify_dzinfo
command	centrify_command
Local Account Management	centrify_local_account_management
Centrify sshd	centrify_sshd
MFA	centrify_mfa

Splunk and Centrify — Better Together

Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Splunk was named a leader in Gartner's 2018 Magic Quadrant for Security Information and Event Management (SIEM) and is positioned as having the most complete vision in the Leaders quadrant.

Centrify, a leading provider of cloud-ready Zero Trust Privilege to secure modern enterprises, has been positioned by Gartner in the Leaders quadrant of the 2018 Gartner Magic Quadrant for Privileged Access Management and has also been named a Leader in The Forrester Wave™: Privileged Identity Management, Q4 2018.

Together, Centrify and Splunk's partnership delivers a streamlined integration for customers who need to identify risks or suspicious activity quickly to remediate threats to their valued assets.

Benefits

- Minimize the risk associated with privileged access to critical data and infrastructure by capturing individual user activity and creating security alerts for quick visibility into suspicious events.
- Centralize visibility across enterprise deployments by correlating privileged access event data with other activity generated across the organization.
- Easily import categorized data sets from privileged activity attributed to the individual into the prescribed SIEM schema for security alert creation.
- Leverage existing investments in SIEM and alert tools without additional costs.

Our mission is to stop the leading cause of breaches – privileged access abuse. Centrify empowers our customers with a cloud-ready Zero Trust Privilege approach to secure access to infrastructure, DevOps, cloud, containers, Big Data and other modern enterprise use cases. To learn more, visit www.centrify.com.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354
sales@centrify.com

Centrify
ZERO TRUST PRIVILEGE