CIMCOR

CimTrak for LogRhythm SIEM by Exabeam

LogRhythm SIEM combined with CimTrak provides the ability to immediately detect and remediate across the enterprise

exabeam

About Exabeam and Cimcor

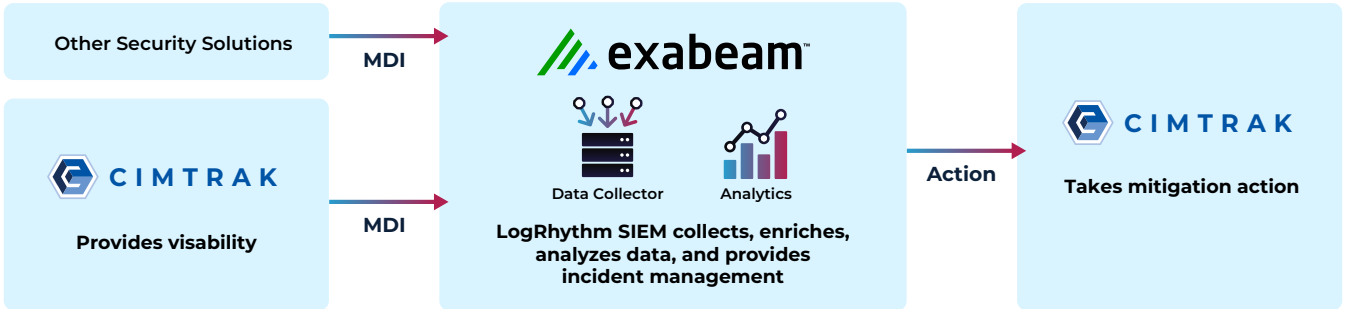
Exabeam and Cimcor work together to help organizations around the globe increase visibility and protect against modern cyberattacks. Exabeam offers extensive support for and integration across Cimcor's product portfolio. The combined solution empowers security teams to identify behavioral anomalies and internal and external threats, then prioritizes their responses based on accurate enterprise security intelligence. Exabeam and Cimcor empower security teams to navigate a changing threat landscape with confidence.

BENEFITS

- Identify security breaches and incidents in seconds compared to an industry average of 207 days
- Remediate and roll back unwanted changes (malicious or circumvented changes) manually or automatically
- Deploy and easily operate in just an hour without the need for professional services
- Gain visibility into unexpected changes to your enterprise

SOLUTION OVERVIEW

CimTrak's integration with LogRhythm SIEM allows it to ingest integrity data that can identify zero-day attacks, ransomware activity, and configuration vulnerabilities, then manually or automatically fix and remove them by rolling back to any number of previously trusted baselines. CimTrak's integration with LogRhythm SIEM provides clear, precise, and actionable data when integrity and compliance drift occur within your infrastructure. CimTrak has a unique capability to manage configurations and reduce change noise by more than 95 percent, thus providing LogRhythm SIEM with concise details of unknown, unwanted, and unexpected activity. Through this integration, LogRhythm SIEM can monitor the integrity of a customer's enterprise, whether those assets are physical, virtual, hybrid, air-gapped, and/or in the cloud. CimTrak works across multiple operating systems and device types, managing files, directories, configurations, users, groups, policies, active directories, database schemas, cloud configurations, hypervisors, containers, network devices, ports, and more.



LOG COLLECTION

Data that gets loaded into a security information and event management (SIEM) platform is what gives it value. There are a lot of noisy data sources that often get categorized as false positives. This is not the case with CimTrak's integration with LogRhythm SIEM, as "integrity" alerts and notifications are high priority and indicate a definitive change in state. If a configuration changed, a port opened, or a file was added that was not authorized, it is indisputable that the change occurred. CimTrak's ability to accomplish this noise reduction is through a workflow process that enables CimTrak to automatically filter out "good" and "authorized" changes, leaving a clear picture of those changes that are either malicious or a violation of your change control process. This process is what enables the detection of zero-day attacks and drives the identification of security incidents from 207 days down to mere seconds.

HOW IT WORKS TODAY

CimTrak has a Syslog parser available for LogRhythm SIEM, which is often the central log aggregator within an enterprise. This allows LogRhythm SIEM to ingest CEF Syslog messages sent from CimTrak. This syslog data is parsed into separate LogRhythm SIEM fields. CimTrak's configuration and change-related information provide powerful detection, awareness, and alerting capabilities regarding the integrity of your critical systems and infrastructure. CimTrak can identify unexpected file changes, file access, systems hardening status, benchmark and compliance scores, STIX/TAXII feeds, threat detection, database changes, active directory changes, baseline changes, firewall changes, ESXi changes, and more! This integration brings all this power and insight directly into LogRhythm SIEM, providing unprecedented visibility for your security operations center (SOC) and network operations center (NOC) and the data needed for forensic investigations.

HOW AUTOMATED WORKFLOW WILL WORK IN THE FUTURE

DATA CLASSIFICATIONS

This will allow every single CimTrak message type to be perfectly mapped to the LogRhythm SIEM classifications allowing all messages to be grouped based on classification. For example, a CimTrak Console Log On Failure will be mapped to LogRhythm SIEM's "Authentication Failure" class.

SMARTRESPONSES

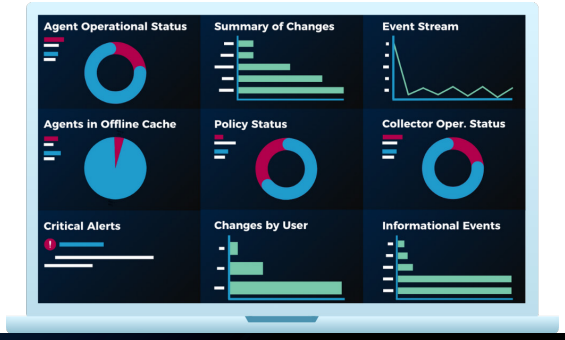
The LogRhythm SmartResponse™ feature lets you execute preventative actions when threat activity is observed. With this integration, CimTrak offers numerous SmartResponse options to help when bad things happen (e.g., trouble ticket generation, rollback, etc).

LOGRHYTHM SMARTRESPONSE ACTIONS FOR CIMCOR

Example	Event	Response
Example 1	A user-identified/selected alert is generated.	CimTrak can revert your baseline back to the previous authoritative version, so you are back to normal.
Example 2	Unauthorized user behavior alert is detected by LogRhythm.	CimTrak can trigger a benchmark scan on that machine to verify its integrity, hardening status, and highlighting any drift from a security standpoint.
Example 3	A new piece if malware is identified, and the file hash of the malware is available.	This file hash can be added to the CimTrak Blocklist to identify if that file is on any monitored system currently (or if it comes up in the future).
Example 4	An update to key systems must be performed and approved files need to be deployed.	The file hashes of the approved files can be added to the CimTrak Allowlist to automatically promote those changes to the baseline and suppress alerting and change noise. This makes it easy to see unexpected changes, even during a system update.
Example 5	A new LogRhythm priority alert has been gathered.	CimTrak can create a ticket in the CimTrak ticketing system (or a third-party ticketing system such as Service Now or BMC Remedy) to document the change or to inform CimTrak of upcoming change requests to automate baseline promotion/management.

LEARN MORE ABOUT CIMTRAK & LOGRHYTHM SIEM

https://www.cimcor.com/partners/exabeam/logrhythm-siem



SUPPORTED PLATFORMS

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS XP, Vista, 7, 8, 10, 11, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise, Windows 11 IoT Enterprise
WINDOWS SERVER 2003, 2008, 2012, 2016, 2019, 2022
LINUX Alma, Amazon, ARM, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, Rocky, SUSE, Ubuntu, others
FREEBSD 12, 13
SUN SOLARIS x86/SPARC
MACOS 5, 6, 7, 8, 9, 10, 11
HP-UX Itanium, PA-RISC
AIX 6.1, 7.1, 7.2, 7.3

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES Compressed, hidden, offline, read-only, archive, reparse point, Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Arista, Aruba, Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Palo Alto, Sophos, others

Supported Platforms CimTrak For Databases

IBM DB2, Microsoft SQL Server, MySQL, Oracle
PARAMETERS MONITORED Default Rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored Procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Amazon AWS, Google Cloud, Microsoft Azure

Supported Container & Orchestration Integrations

Amazon Elastic Kubernetes Service (EKS), Docker, Docker Enterprise, Google Kubernetes Engine (GKE), Kubernetes, Podman

Supported Ticketing Integrations

Atlassian Jira, BMC Remedy, CA ServiceDesk, ServiceNow

Supported SIEM Integrations

IBM QRadar, LogRhythm, McAfee Event Security Manager, Microfocus Arcsight, Splunk, others

Supported Under CimTrak's Trusted File Registry™

CentOS 7, Microsoft Windows 7, 8, 8.1, 10, 11, XP, 2003, 2008, 2012, 2016, 2019, 2022, Oracle Linux 7, Redhat Enterprise Linux 7

SUPPORTED BENCHMARKS

ALIBABA
ALMA
AMAZON ELASTIC KUBERNETES
AMAZON LINUX
APACHE
APPLE MAC OS
AZURE
CENTOS
CISCO Firewall, IOS
DEBIAN
DISTRIBUTION INDEPENDENT
FEDORA
GOOGLE Chrome, Container, Kubernetes
IBM
KUBERNETES
MICROSOFT Access, Edge, Excel, IIS, Intune, Office, PowerPoint, SharePoint, SQL, Windows, Windows Server, Word
MONGODB
NGINX
ORACLE Cloud, Database, Linux, MySQL
PALO ALTO
POSTGRESQL
RED HAT
RHEL8
ROCKY
ROS
SUSE
UBUNTU LXD, Linux
VMWARE

REQUEST A DEMO

exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

CIMCOR

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.

CIMCOR.COM | FOLLOW US @CIMTRAK

CIMTRAK