Feature Brief

# Streamline Your Workflow with Detail Page

## Harness Your SIEM Data in a Single View to Reduce Mean Time to Respond (MTTR)

Your data offers a wealth of information, but understanding it all is challenging and time consuming, and you don't have time to spare. Get to the story your data is telling faster with LogRhythm's Detail Page. As part of the LogRhythm NextGen SIEM Platform, Detail Page gives you a better understanding and visualization of what's happening in your environment with users and hosts. Detail Page shows you what happened before and after a threat or anomaly occurred and helps you analyze the impact to reduce your mean time to respond.

## Real-Time Visibility into Data with Detail Page

To detect threats, your team needs full visibility to investigate and take immediate action. Detail Page creates a security story with your log data and presents it in a single view, eliminating the need to dig into logs or search through multiple pages or products.

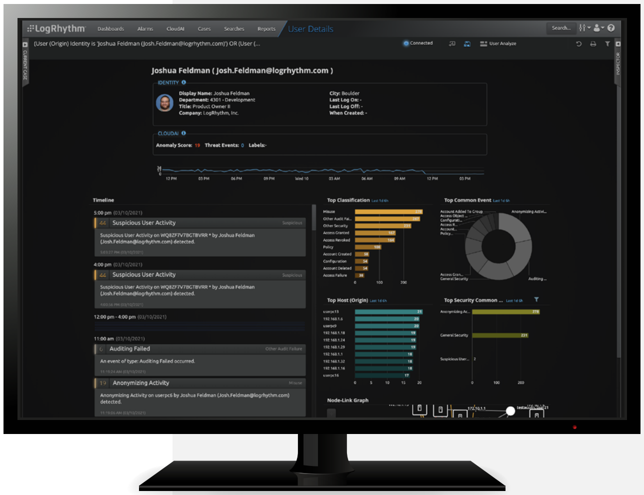
Detail Page lets your team build custom layouts and investigatively drill down into real-time data derived from both machine learning and scenario-based analytics. Unlike other solutions, LogRhythm's Detail Page acts as a single pane of glass for users and hosts, enabling you to quickly understand incident timing and scope. User and host information is populated using LogRhythm's TrueIdentity™ and TrueHost, which map disparate user and host accounts and related identifiers together, so there is no confusion about what's occurring in your environment.

Detail Page also saves you time, allowing you to pivot seamlessly between users and hosts to boost your investigations. Initiate your response directly from the Detail Page with easy access to SmartResponse™ automation plugins and Case Management.

## See Detail Page in Action

To understand what's occurring in your network, it's important to see the full picture. Click below to see how Detail Page helps you piece together the security story and presents log data in a single view, helping you make faster decision and lower your response time.

Watch the Demo ⟶



(User (Origin) Identity is 'Joshua Feldman (Josh.Feldman@logrhythm.com)') OR (User (...

Joshua Feldman ( Josh.Feldman@logrhythm.com )

IDENTITY

Display Name: Joshua Feldman
Department: 4301 - Development
Title: Product Owner II
Company: LogRhythm, Inc.
City: Boulder
Last Log On: -
Last Log Off: -
When Created: -

CLOUDAI

Anomaly Score: 19 Threat Events: 0 Labels:-

Timeline

5:00 pm (03/10/2021)
44 Suspicious User Activity — Suspicious
Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.
5:03:27 PM (03/10/2021)

4:00 pm (03/10/2021)
44 Suspicious User Activity — Suspicious
Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.
4:00:56 PM (03/10/2021)

12:00 pm - 4:00 pm (03/10/2021)

11:00 am (03/10/2021)
6 Auditing Failed — Other Audit Failure
An event of type: Auditing Failed occurred.
11:19:24 AM (03/10/2021)

19 Anonymizing Activity — Misuse
Anonymizing Activity on userpc6 by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.
11:19:06 AM (03/10/2021)

## Benefits

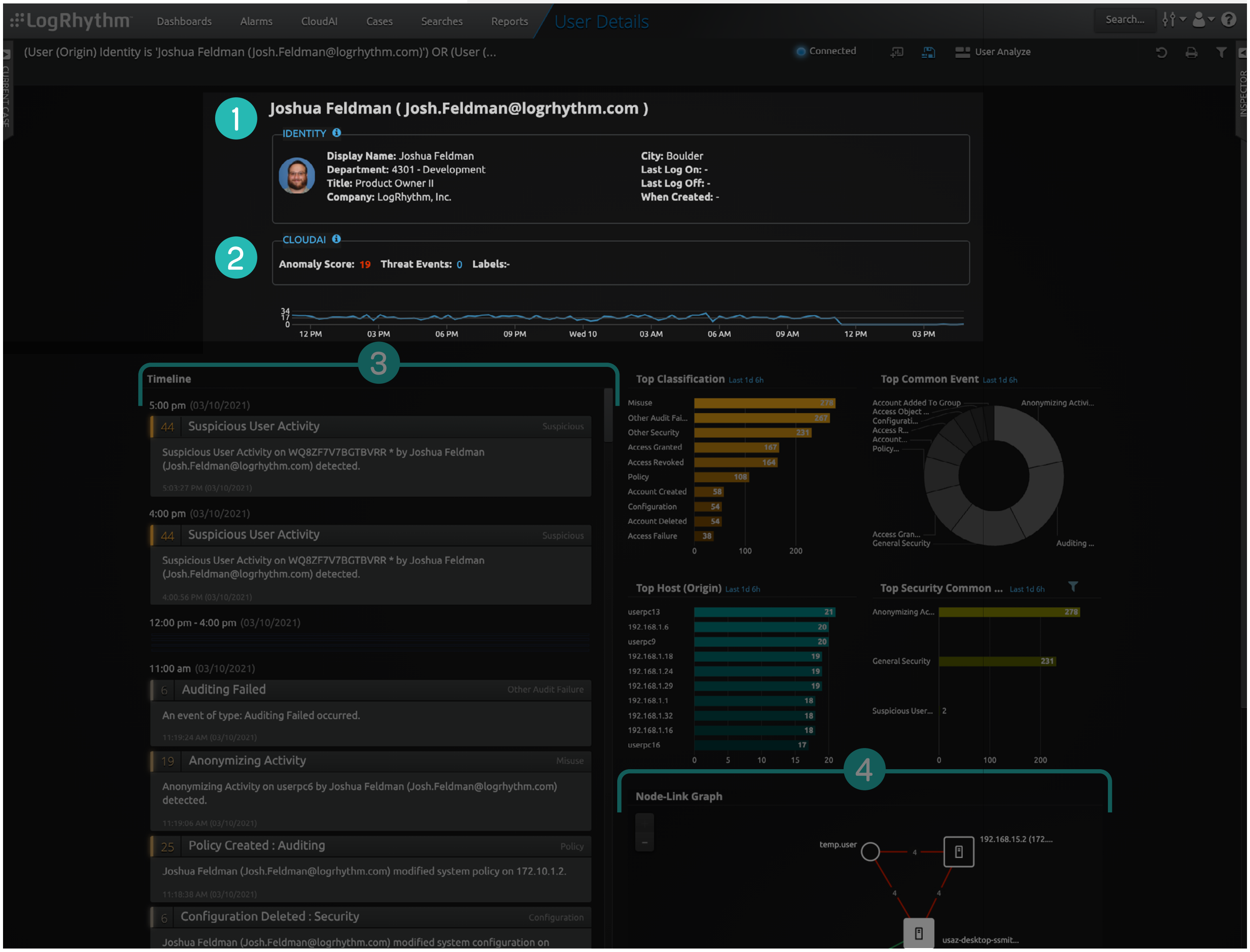
- Faster detection and threat response
- Easy-to-understand security story
- Simplified correlation of users, hosts, and events
- Convenient drill down from security story to raw data

## Detail Page Answers:

- Which user or host was affected by the incident?
- What was the activity before and after the incident?
- Was the activity normal behavior?
- What other users or hosts may be affected?

# Detail Page Overview

1 TrueIdentity or TrueHost   2 CloudAI   3 Timeline View   4 Node-Link Graph



(User (Origin) Identity is 'Joshua Feldman (Josh.Feldman@logrhythm.com)') OR (User (...

Joshua Feldman ( Josh.Feldman@logrhythm.com )

IDENTITY

**Display Name:** Joshua Feldman
**Department:** 4301 - Development
**Title:** Product Owner II
**Company:** LogRhythm, Inc.

**City:** Boulder
**Last Log On:** -
**Last Log Off:** -
**When Created:** -

CLOUDAI

**Anomaly Score:** 19 **Threat Events:** 0 **Labels:**-

Timeline

5:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious

Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

5:03:27 PM (03/10/2021)

4:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious

Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

4:00:56 PM (03/10/2021)

12:00 pm - 4:00 pm (03/10/2021)

11:00 am (03/10/2021)

6 Auditing Failed — Other Audit Failure

An event of type: Auditing Failed occurred.

11:19:24 AM (03/10/2021)

19 Anonymizing Activity — Misuse

Anonymizing Activity on userpc6 by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

11:19:06 AM (03/10/2021)

25 Policy Created : Auditing — Policy

Joshua Feldman (Josh.Feldman@logrhythm.com) modified system policy on 172.10.1.2.

11:18:38 AM (03/10/2021)

6 Configuration Deleted : Security — Configuration

Joshua Feldman (Josh.Feldman@logrhythm.com) modified system configuration on

## 1 Obtain Accurate Analytics with TrueIdentity and TrueHost

LogRhythm's TrueIdentity associates multiple account identifiers and types to a single identity construct. TrueIdentity allows machine analytics to take into account all of the activities from the same user, regardless of account type or how the account is represented in log data. Meanwhile, LogRhythm TrueHost associates multiple host identifiers, such as IP address, hostname, and MAC address to the same host, offering a more comprehensive understanding of activities from the same host. Understanding all of the activities generated by the same user or host enables more accurate analytics to determine security relevant events.

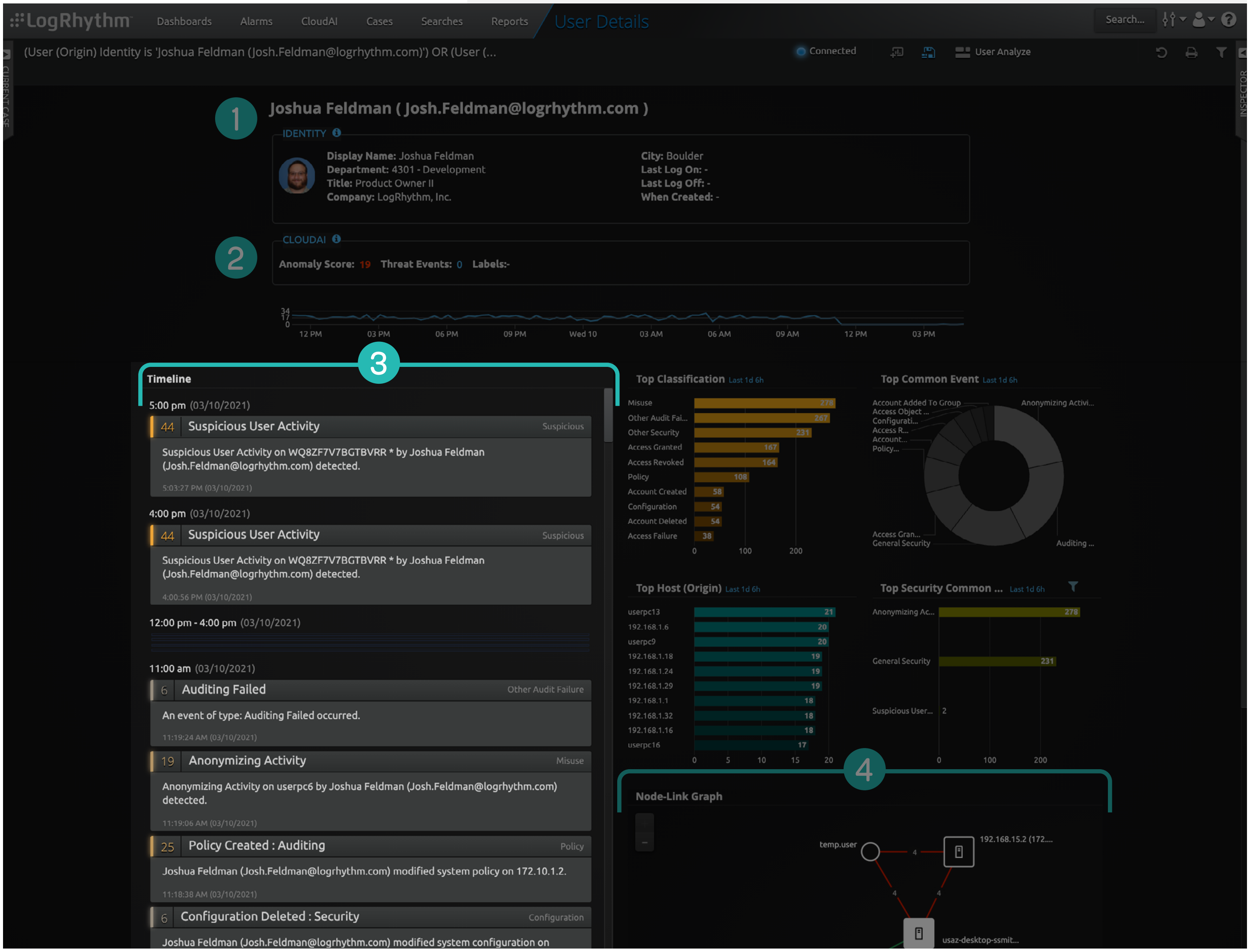
See It in Action ⟶

## 2 Uncover User Behavior with CloudAI

If enabled, behavioral data appears on the Detail Page, showing an anomaly score, the number of threat events, as well as CloudAI labels about the user or host. This indicates machine learning analytics surfaced an insight about a user and the user's behavior, helping you spot important events. These insights provide valuable context that determine the impact and help you understand if the activity you're seeing is typical or if it warrants further investigation.

See It in Action ⟶

1 TrueIdentity or TrueHost 2 CloudAI 3 Timeline View 4 Node-Link Graph



Joshua Feldman ( Josh.Feldman@logrhythm.com )

IDENTITY

**Display Name:** Joshua Feldman
**Department:** 4301 - Development
**Title:** Product Owner II
**Company:** LogRhythm, Inc.

**City:** Boulder
**Last Log On:** -
**Last Log Off:** -
**When Created:** -

CLOUDAI

**Anomaly Score:** 19 **Threat Events:** 0 **Labels:**-

Timeline

5:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious

Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

5:03:27 PM (03/10/2021)

4:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious

Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

4:00:56 PM (03/10/2021)

12:00 pm - 4:00 pm (03/10/2021)

11:00 am (03/10/2021)

6 Auditing Failed — Other Audit Failure

An event of type: Auditing Failed occurred.

11:19:24 AM (03/10/2021)

19 Anonymizing Activity — Misuse

Anonymizing Activity on userpc6 by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

11:19:06 AM (03/10/2021)

25 Policy Created : Auditing — Policy

Joshua Feldman (Josh.Feldman@logrhythm.com) modified system policy on 172.10.1.2.

11:18:38 AM (03/10/2021)

6 Configuration Deleted : Security — Configuration

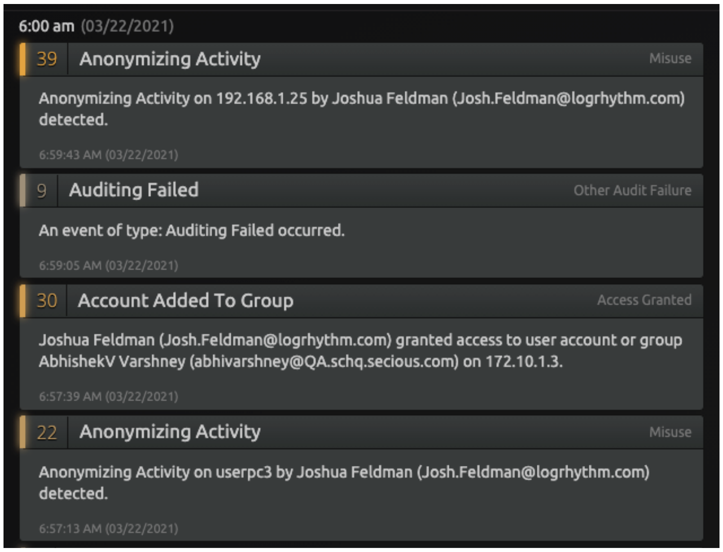
Joshua Feldman (Josh.Feldman@logrhythm.com) modified system configuration on

## 3 Speed Threat Detection and Response with Timeline View

Embedded within the Detail Page is the Timeline View widget, which presents user and host activity chronologically and highlights key events to filter out the "noise." Each view shows the dynamic risk-based prioritization (RBP) value assigned to machine data that helps you identify important events. With Timeline View, you can see the progression of a threat over time, helping you make decisions faster and execute an immediate response.

Unlike other competitive solutions, you can display any data with LogRhythm's Timeline View widget. Timeline View is also user configurable. Filter the data and select what you want to appear to customize your view.

See It in Action ⟶



6:00 am (03/22/2021)

39 Anonymizing Activity — Misuse

Anonymizing Activity on 192.168.1.25 by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

6:59:43 AM (03/22/2021)

9 Auditing Failed — Other Audit Failure

An event of type: Auditing Failed occurred.

6:59:05 AM (03/22/2021)

30 Account Added To Group — Access Granted

Joshua Feldman (Josh.Feldman@logrhythm.com) granted access to user account or group AbhishekV Varshney (abhivarshney@QA.schq.secious.com) on 172.10.1.3.

6:57:39 AM (03/22/2021)

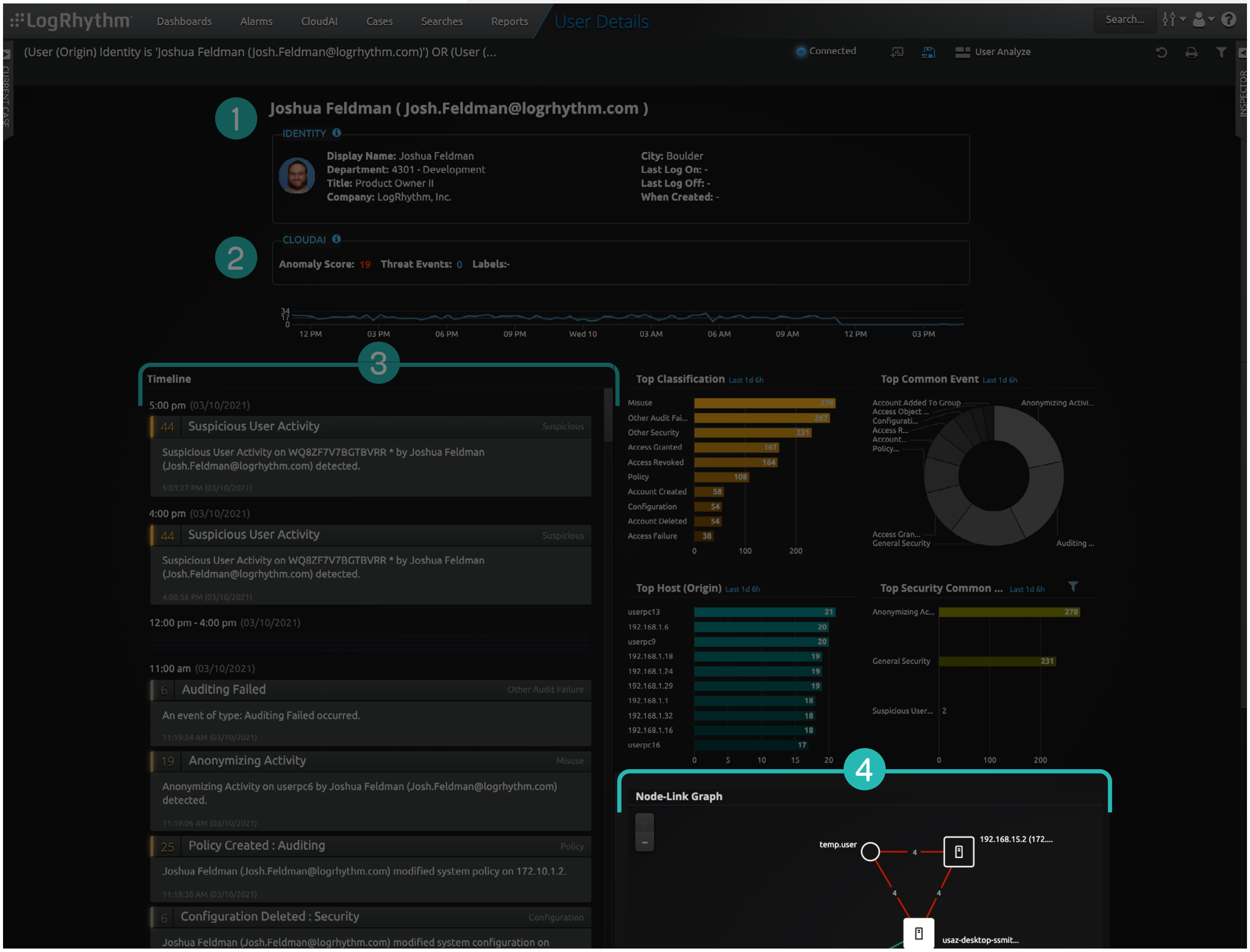
22 Anonymizing Activity — Misuse

Anonymizing Activity on userpc3 by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

6:57:13 AM (03/22/2021)

Figure 1: Timeline View shows a sequence of events with risk-based prioritization scores

1 TrueIdentity or TrueHost  2 CloudAI  3 Timeline View  4 Node-Link Graph



(User (Origin) Identity is 'Joshua Feldman (Josh.Feldman@logrhythm.com)') OR (User (...

Joshua Feldman ( Josh.Feldman@logrhythm.com )

IDENTITY

**Display Name:** Joshua Feldman
**Department:** 4301 - Development
**Title:** Product Owner II
**Company:** LogRhythm, Inc.

**City:** Boulder
**Last Log On:** -
**Last Log Off:** -
**When Created:** -

CLOUDAI

**Anomaly Score:** 19 **Threat Events:** 0 **Labels:**-

Timeline

5:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious

Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

5:03:27 PM (03/10/2021)

4:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious

Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

4:00:56 PM (03/10/2021)

12:00 pm - 4:00 pm (03/10/2021)

11:00 am (03/10/2021)

6 Auditing Failed — Other Audit Failure

An event of type: Auditing Failed occurred.

11:19:24 AM (03/10/2021)

19 Anonymizing Activity — Misuse

Anonymizing Activity on userpc6 by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.

11:19:06 AM (03/10/2021)

25 Policy Created : Auditing — Policy

Joshua Feldman (Josh.Feldman@logrhythm.com) modified system policy on 172.10.1.2.

11:18:38 AM (03/10/2021)

6 Configuration Deleted : Security — Configuration

Joshua Feldman (Josh.Feldman@logrhythm.com) modified system configuration on

Top Classification Last 1d 6h

| | |
|---|---|
| Misuse | 278 |
| Other Audit Fai... | 267 |
| Other Security | 231 |
| Access Granted | 167 |
| Access Revoked | 164 |
| Policy | 108 |
| Account Created | 58 |
| Configuration | 54 |
| Account Deleted | 54 |
| Access Failure | 38 |

Top Common Event Last 1d 6h

Top Host (Origin) Last 1d 6h

| | |
|---|---|
| userpc13 | 21 |
| 192.168.1.6 | 20 |
| userpc9 | 20 |
| 192.168.1.18 | 19 |
| 192.168.1.24 | 19 |
| 192.168.1.29 | 19 |
| 192.168.1.1 | 18 |
| 192.168.1.32 | 18 |
| 192.168.1.16 | 18 |
| userpc16 | 17 |

Top Security Common ... Last 1d 6h

| | |
|---|---|
| Anonymizing Ac... | 278 |
| General Security | 231 |
| Suspicious User... | 2 |

Node-Link Graph

## 4 Determine Incident Scope with Node-Link Graph

LogRhythm's Node-Link Graph provides a visual representation of how hosts and users connect to each other within the data, surfacing relationship data in logs. The Node-Link Graph feature appears on the Detail Page to help you identify patterns and abnormalities present in log data.

LogRhythm's Machine Data Intelligence (MDI) Fabric supplements the graph with contextual data to explain the relationship and type of activity occurring between connections. Node-Link Graph lets you filter data and quickly identify unusual network traffic between hosts and users, relationships of interest, and abnormalities.

See It in Action ⟶

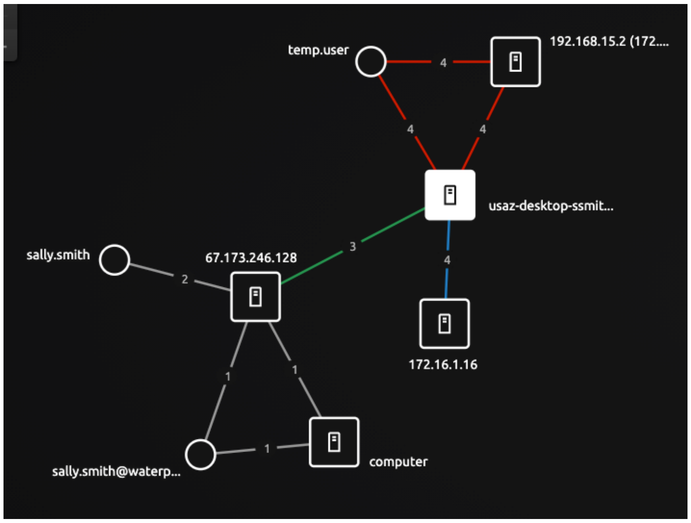
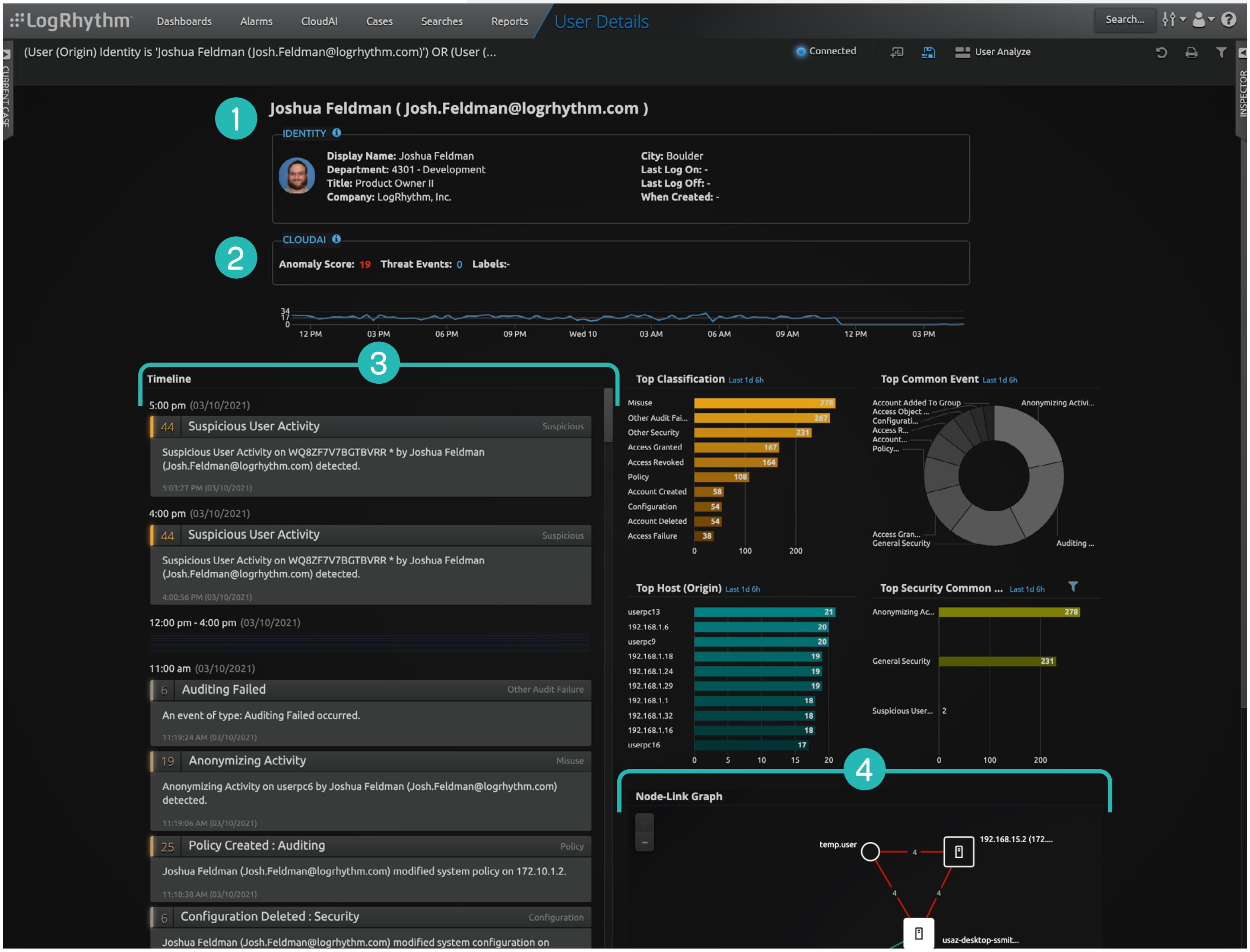


Figure 2: Node-Link Graph helps you surface relationships between log data

1 TrueIdentity or TrueHost 2 CloudAI 3 Timeline View 4 Node-Link Graph



(User (Origin) Identity is 'Joshua Feldman (Josh.Feldman@logrhythm.com)') OR (User (...

Joshua Feldman ( Josh.Feldman@logrhythm.com )

IDENTITY

**Display Name:** Joshua Feldman
**Department:** 4301 - Development
**Title:** Product Owner II
**Company:** LogRhythm, Inc.

**City:** Boulder
**Last Log On:** -
**Last Log Off:** -
**When Created:** -

CLOUDAI

**Anomaly Score:** 19 **Threat Events:** 0 **Labels:**-

Timeline

5:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious
Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.
5:03:27 PM (03/10/2021)

4:00 pm (03/10/2021)

44 Suspicious User Activity — Suspicious
Suspicious User Activity on WQ8ZF7V7BGTBVRR * by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.
4:00:56 PM (03/10/2021)

12:00 pm - 4:00 pm (03/10/2021)

11:00 am (03/10/2021)

6 Auditing Failed — Other Audit Failure
An event of type: Auditing Failed occurred.
11:19:24 AM (03/10/2021)

19 Anonymizing Activity — Misuse
Anonymizing Activity on userpc6 by Joshua Feldman (Josh.Feldman@logrhythm.com) detected.
11:19:06 AM (03/10/2021)

25 Policy Created : Auditing — Policy
Joshua Feldman (Josh.Feldman@logrhythm.com) modified system policy on 172.10.1.2.
11:18:38 AM (03/10/2021)

6 Configuration Deleted : Security — Configuration
Joshua Feldman (Josh.Feldman@logrhythm.com) modified system configuration on

## The LogRhythm Difference

LogRhythm delivers powerful investigative tools to correlate attack indicators from different security silos. Our platform lets you access the timeline of events, user and host relationships, aggregate metadata, and the raw event data all within the Detail Page. When combined with LogRhythm's MDI Fabric, you can easily understand what you are looking at and take action.

LogRhythm's Detail Page saves you time from switching views to decipher the data. Our curated security narrative and MDI Fabric provide an accurate and complete picture of your data, empowering you to make better decisions, reduce your organizational risk, and quickly resolve security incidents.

To learn more about LogRhythm, schedule a custom demo.

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301 www.logrhythm.com