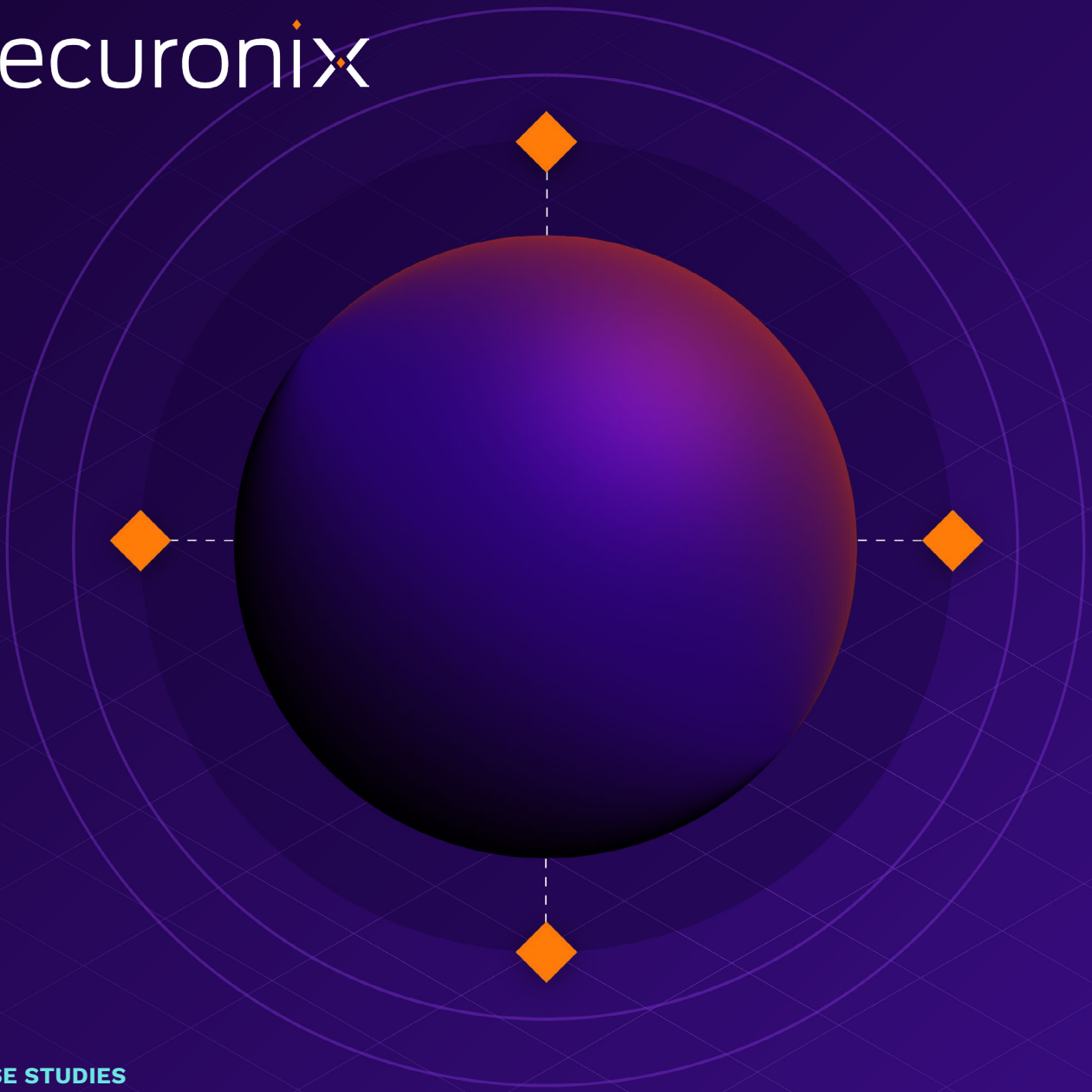
securonix



CASE STUDIES

# Insider Threat Detection & Response

# Securonix for Insider Threat Detection & Response

Insider threats are becoming more frequent and costly, in fact, 60% of data breaches now involve insiders*. Insiders already have access to valuable company information and may regularly access it as a part of their job. This access can pose a huge risk when left unchecked and unmonitored. Using advanced behavioral analytics, we can help you identify and investigate when user access patterns deviate from normal, baseline behaviors indicating a possible insider threat.

## Our Approach

Securonix's AI-Reinforced Unified Defense SIEM platform, inclusive of our proven UEBA solution, gives you complete visibility into threats from users and entities, both inside and outside of your organization. Our out-of-the-box content covers common insider threat use cases such as data exfiltration, privilege account abuse and misuse, compromised users, and more. The agnostic architecture of Securonix UEBA means it can even sit on top of your existing SIEM, reducing false positives and helping you detect insider threats with identity context across your ecosystem.

*idwatchdog.com

cencora


# Cencora Uses Securonix Unified Defense SIEM to Reduce Cyber Risk by 80%

## The Challenge

As one of the world's largest pharmaceutical distributors, Cencora (formerly AmerisourceBergen), needed to find a cybersecurity solution that could ingest and analyze all of the data across their huge IT environment. They needed an option that was both cost-effective at scale and could detect potential threats both within and outside their organization.

## The Solution

Securonix provided analytics on an open and cost-effective platform that can ingest huge volumes of data from their over 100 devices that generate over 100 billion events. Using our AI-Reinforced, Unified Defense SIEM solution, Cencora now has the context needed to identify and respond to malicious insider behaviors at scale.

## Business Impact

- Detected and resolved 400 insider threats within the first month.
- Gained visibility into the kill chain to identify which threats needed to be prioritized.
- Helped them meet compliance goals with coverage across HIPAA, PCI, DSS and GDPR.

Read the full story

GOLOMT BANK

# Securonix Helps Golomt Bank Detect Cyber and Insider Threats

## The Challenge

Golomt Bank lacked centralized visibility with their previous on-prem solution and needed better scalability and analytics as their organization matured. They needed a scalable SIEM that could detect complex insider threats and alert them when their employees were deviating from baseline behaviors.

## The Solution

With Securonix's Unified Defense SIEM, they now have zero infrastructure to manage and holistic and consolidated visibility into their entire environment. The bank uses Securonix AI-Reinforced SIEM to detect threats at scale, ingesting huge volumes of data, including from custom data sources. Their security team can now monitor cloud data for misuse or compromise within their environment.

## Business Impact

- Achieved huge cost savings and valuable insights into user behavior with built-in UEBA capabilities.
- Moved to the cloud to achieve fast time-to-value and zero infrastructure to manage.
- Gained full visibility of their data across cloud, on-prem, and hybrid sources.

Read the full story

# PROFESSIONAL SERVICES

## Identify and Detect Data Exfiltration in the Professional Services Industry

### The Challenge

A large consulting organization needed to assess their security posture and ensure the large amount of sensitive customer data they handled was safe from unknown threats hiding in their environment. Building an insider threat program was crucial to their security goals and their chief risk advisor was tasked with starting an insider threat program.

### The Solution

Leveraging Securonix UEBA, the organization gained insight into correlations between user behavior and data movement. They were able to customize user risk scoring to help them prioritize and mitigate potential risks caused by negligent and malicious users while also employing granular Role-based Access Control (RBAC) to ensure sensitive identities remained anonymous until unmasking was required.

### Business Impact

- Decreased false positives from 30% to only 10% of all alerts.
- Lowered the average incidents that needed investigating to 30 per week for a workforce of over 80,000 employees.
- Discovered majority of threats were non-malicious, and implemented security training for staff.

Read the full story

# HOLDING COMPANY

## Holding Company Stops Phishing and Data Exfiltration with a Single Platform

### The Challenge

A large holding company needed to centralize their security efforts across their business units but lacked visibility across their security tools. They wanted to detect and respond to phishing emails but lacked behavioral analytics to detect insider and advanced threats.

### The Solution

Using Securonix's Unified Defense SIEM powered by industry leading UEBA, their SOC was able to detect and respond to their biggest threat – phishing. Leveraging a custom two-policy setup, they can detect an attack that utilizes free domain trial accounts. With these policies, the security team can shut down these sophisticated attacks – something no other SIEM vendor could help them accomplish.

### Business Impact

- Gained centralized visibility across all of their business units.
- Leveraged OOTB policies to detect data exfiltration attempts they were blind to previously.
- Increased security posture with a two-policy setup that focused on looking for newly registered domains.

Read the full story

# Testimonial

“Securonix is a good SIEM product to detect anomalies and secure your environment from known cyber threats. The Behavioral Analytics-based use cases have helped us identify both malicious insiders and intruders in our network.”

- Cybersecurity Engineer at Large Healthcare Organization

## Why Choose Securonix for Insider Threats?

Securonix analyzes diverse users, entities, systems, applications, security events, and physical access data to identify high-risk behavior and help analysts prioritize and investigate high-risk incidents.

- Shorten the time required to detect and respond to insider threats from malicious and negligent employees.
- Rapidly identify high risk users, including risky activities like data exfiltration, privilege account abuse and misuse, and compromised users.
- Streamline threat hunting for hard-to-find threats already in your network.

To learn how Securonix helps uncover insider threats, Request a Demo.

securonix