sumo logic

# DXL ditches on-prem SIEM for modern, cloud-native security solution

## Results at a glance

- → 50-100 access denied errors per minute detected and resolved through log correlation
- → Real-time insights at their fingertips through out-of-the-box and custom dashboards
- → Log analysis time slashed from five minutes to seconds
- → Faster threat detection and investigation with contextual search and built-in threat intelligence
- → Consolidated disparate tools into one centralized Cloud SIEM platform for streamlined security operations and analysis

DXL
BIG + TALL

**PRODUCTS**

Cloud SIEM

**USE CASES**

Threat detection, investigation, and response

**ENVIRONMENT**

AWS

Microsoft Azure

## Challenge

### Managing their on-premises infrastructure was slowing DXL down. They were looking for a cloud-native SIEM that could properly handle their growing environment.

As a lean team of five engineers, DXL's security team was stretched thin maintaining their former on-premises SIEM solution, LogRhythm. Manual product updates occasionally triggered system downtime, storage limitations restricted data retention, and troubleshooting hardware issues fell on their shoulders. As the business scaled and adopted more modern, cloud-based services, their on-premises tooling couldn't keep up.

John Sacchetti, Director of Cybersecurity and Networking at DXL, knew they needed a cloud-native SIEM. The team needed a SIEM that could scale alongside them, consolidate fragmented tools, and support them on their journey to modernized, secure operations.

DXL BIG + TALL

**INDUSTRY**

Retail

**ABOUT**

Destination XL Group (DXL) sells moderately-priced, private-label and name-brand casual wear, dresswear, and suits for big-and-tall men at about 420 Casual MaleXL and Outlet stores in 45 US states, as well as online and through catalogs.

**WEBSITE**

dxl.com

## Solution

On his search for a new SIEM solution, Sacchetti wanted a tool that drastically shortens log analysis time, helps them act faster, and integrates seamlessly with their growing ecosystem of third-party tools. After evaluating Google Security Operations, Splunk, and other SIEM platforms, he found the solution in Sumo Logic Cloud SIEM.

### Seamless third-party integration in one, centralized platform

Given their large number of third-party tools and ongoing investments in new technologies, a platform that could integrate and centralize data from multiple sources was their top priority.

Sumo Logic stood out for its ability to ingest, correlate, and analyze logs from diverse platforms. Sacchetti wanted to ensure that critical systems, including their main content delivery network (CDN), Akamai, as well as authentication tools like Azure AD, AWS, and other platforms, could easily feed data into a single platform for real-time monitoring and threat detection.

"As we continuously change our business and add new services for our customers, website updates, and different integrations to produce sales, with the power of Sumo Logic within our toolbox, we're confident that we can ingest, report, and search logs, as well as build reporting from any of those third parties, whether they're currently supported or not by Sumo Logic because we can throw anything at it and normalize the data," notes Sacchetti.

## Simplified PCI compliance with built-in apps

One of DXL's requirements was a solution that could make meeting regulatory requirements easier without adding extra burden. Sumo Logic's built-in PCI compliance applications were a key reason they chose the platform. "We have to maintain PCI compliance like the big players, but we don't have the same resources. Sumo Logic helps us bridge that gap."

With out-of-the-box dashboards covering Microsoft Windows logs, AWS logs, firewall events, and more, Sacchetti's team can easily detect potential compliance issues, such as unusual inbound or outbound traffic or unauthorized server access, without manual effort.

## Out-of-the-box and custom dashboards

When evaluating different SIEM solutions, Sacchetti valued ease of use and flexibility in dashboarding. They needed a tool that could support both out-of-the-box dashboards and custom views tailored to their unique needs, and Sumo Logic provided that. When executives ask for specific data, they can pull real-time insights on the fly without fumbling between multiple tools or manually stitching information together.

**CUSTOMER EXPERIENCE**

"The ability to have Sumo Logic already do the heavy lifting and the dirty work for us, such as the dashboarding and field distraction rules, is a big win for us as it relieves our workload and allows us to communicate security insights more effectively across the business.

**John Sacchetti**
**Director of Cybersecurity and Networking**
DXL

Whether someone needs log data from a specific platform or a high-level view of security metrics, DXL's security team could quickly generate reports in an easy-to-understand format and even customize the findings based on people's preferences and priorities.

Sacchetti appreciated how Sumo Logic managed to take anything they threw at it: "The ability to have Sumo Logic already do the heavy lifting and the dirty work for us, such as the dashboarding and field distraction rules, is a big win for us as it relieves our workload and allows us to communicate security insights more effectively across the business."

**BY THE NUMBERS**

**5 min → seconds**

accelerated log analysis

## Results

### Real-time insights cut log analysis from five minutes to seconds

With Sumo Logic, DXL's security team greatly reduces the time it takes to gather and deliver critical insights for internal teams and stakeholders. With everything centralized in Sumo Logic, they can quickly run searches, generate reports, and customize dashboards with a snap of a finger.

Logs that took five minutes to appear in their SaaS platforms' visualizations now show up instantly. Rather than dealing with delays, the team can spot issues and respond in seconds, which is a game-changer when every moment counts in security.

"We're able to shortcut a lot of the analysis," Sacchetti said. "Having everything as a source of truth in Sumo Logic allows us to pull data, save searches, and easily tweak them for different requests, without starting from scratch every time."

### Efficient log search and correlation

With their previous setup, log search and analysis were time-consuming. They had to dig through various tools to investigate potential threats that would otherwise go unnoticed, but now it's a breeze with Sumo Logic.

Sacchetti says, “With just a few clicks, we can detect if there’s any attempted attack traffic happening, where users are going, or where the traffic lies. When we look at how much traffic is going in through our CDN, that correlation piece within the log search is huge and has become the number one feature we use often.”

### 50 to 100 access denied errors per minute caught and resolved

Sumo Logic’s Logs for Security helps them detect and resolve misconfigurations that may have gone unnoticed and lead to a larger security incident. The team uncovered a misconfiguration within their AWS CloudTrail logs, generating 50 to 100 “access denied” errors per minute, something that would’ve been difficult for them to identify manually due to their small team size.

Sacchetti can easily detect unusual patterns using the solution, as “Sumo Logic acts as an auditor for us to find misconfigurations and other potential security incidents.”

Beyond access denied errors, the ability to detect traffic fluctuations or error spikes helps the team determine whether something is malicious or simply a setup issue. By addressing problems early, DXL not only strengthens security but also avoids unnecessary cloud costs tied to inefficient processes.

### Faster threat investigation with contextual search and integrations

Sacchetti is laser-focused on detecting potential threats by contextually searching IP addresses, which they achieve using Sumo Logic Cloud SIEM. With built-in integrations to services like VirusTotal and AbuseIPDB, they can instantly assess the reputational value of suspicious IPs.

They can make faster decisions, such as blocking malicious traffic, without having to manually search across multiple tools. Sacchetti highlights that this feature streamlines investigations and could even be automated further via Sumo Logic’s API and their firewall.

**CUSTOMER EXPERIENCE**

With just a few clicks, we can detect if there’s any attempted attack traffic happening, where users are going, or where the traffic lies. When we look at how much traffic is going in through our CDN, that correlation piece within the log search is huge and has become the number one feature we use often.

**John Sacchetti**
**Director of Cybersecurity and Networking**
DXL

### Simplified security operations due to tool consolidation

Before Sumo Logic, DXL's security team had to juggle multiple tools to correlate logs, track group policy changes, and monitor user or group modifications across both on-premises and cloud environments.

Now, with everything centralized in Sumo Logic, their team has a single source of truth for security analysis and investigations.

### Continuous customer support and partnership

Beyond the technology itself, Sacchetti emphasizes the customer support they've received from Sumo Logic ever since they first invested in the solution. From onboarding to day-to-day operations, Sacchetti notes that the Sumo Logic customer success team remains responsive and invests in DXL's success.

Seasoned and newer team members alike are given free tools to learn and grow within Sumo Logic, such as the Sumo Logic certification program and monthly brown bag sessions, which help the team become more familiar with the product.

> "There hasn't been anything I've thrown at Sumo Logic that it couldn't handle. No matter how simple or complex the tech stack, it ingests, normalizes, and reports on the data exactly how we need it, making our lives a whole lot easier. And the support we've received along the way has been some of the best I've seen from any partnership I've had with any product I use.

John Sacchetti
Director of Cybersecurity and Networking
DXL

Read more about other customer successes — from retail to healthcare to fintech here.

**Learn More**
Toll-Free: 1.855.LOG.SUMO | Int'l: 1.650.810.8700

sumologic.com



855 Main Street, Redwood City, CA 94603