Respond to a potential M365 cyber attack in minutes instead of hours

About the customer

A Canadian company with significant investments in the energy and utilities sector, including power generation, natural gas distribution, and electricity transmission. It has also diversified into real estate and transportation.

About CoreView

The CoreView Microsoft 365 Management Platform helps IT teams get full value from their Microsoft 365 investment. With more than 15 years of experience and over 25 million users, CoreView is trusted by IT and security leaders around the world.

The challenge

When Suncor was struck by a cyber attack so severe that it temporarily shut them down completely, information about the situation circulated fast throughout the industry.

The Canadian Cyber Partnership sent out alerts and information to all organizations working with Suncor warning of potential danger.

One of the leading Canadian natural gas distributors started taking action. Since email is a major attack vector, they wanted to be able to quickly audit their Microsoft Exchange mailboxes to find any potential exposure. Luckily, they were a CoreView customer.

The solution

While an audit of this nature could take days or weeks, the IT team did it in minutes using the Microsoft 365 audit tools from CoreView. They quickly identified risk areas and began taking countermeasures.

"CoreView's audit capabilities made the incident response process effortless. In minutes we were able to rapidly zero in on critical data that would normally take weeks to uncover."

– Spokesperson for the Canadian Company

CoreView's M365 audit tools lead to immediate action

The first step for assessing the organization's risk level was to locate all emails that any of their team had recently sent to Suncor during the cyber attack. Then, they needed to pinpoint who sent them and when.

With CoreView's Microsoft 365 audit tools, this entire process became easy, allowing the organization to conduct the audit in minutes.

"CoreView's audit capabilities made the incident response process effortless. In minutes we were able to rapidly zero in on critical data that would normally take weeks to uncover," a spokesperson for the organization said.

They then followed up on their internal email accounts to ensure no security breach occurred.

Identified and removed suspicious M365 guest access in bulk

After the audit, upper management was still concerned about a potential breach and asked the IT team to take further action.

Using CoreView's Guest Accounts report, the team searched for guest account activity in Microsoft 365 from the originally affected company.

They then filtered the data to identify any suspicious M365 accounts.

Then, within the report, the team removed all Microsoft 365 guest accounts and blocked their M365 credentials in bulk.

The result? Effective incident response for Microsoft.

The impact

In the end, CoreView's tools **saved the company hours of response time** during a critical moment. The platform empowered the company's IT team to take proactive steps to ensure they did not suffer the same fate as the other company.

To learn more about CoreView's customers, visit www.coreview.com/our-customers