CASE STUDY

Municipality exercises caution over suspicious EDR alerts

INDUSTRY

State Level Government - Local Government

EMPLOYEES

1,000+

COVERAGES

Breach Response

Something just wasn't right. A municipality began noticing suspicious activity from Endpoint Detection and Response (EDR) alerts. They couldn't discern what was happening but were concerned they were looking at the start of ransomware activity. So they took caution, shut down their network, and called Coalition's Claims hotline late that evening.

Upon the scoping call, an investigation was set up early the following morning. The municipality's Breach Response coverage kicked in, and Coalition Incident Response (CIR) got to work immediately to investigate the activity. Within 48 hours of the initial call to Coalition, CIR helped the municipality get its systems back up and running.

In the meantime, our Claims team helped the municipality proactively prepare a communication strategy for both employees and residents affected by the possible attack. In less than two weeks, CIR wrapped up its investigation and determined there was no malicious activity in the municipality's network. From there, CIR assisted them with configuration changes to their EDR so they wouldn't see the confusing information in the future.

Every minute counts if there's a threat actor in your network. It was a cautious (and smart) move by this municipality to reach out to Coalition and shut down their systems the moment they detected suspicious activity. Because they had Breach Response coverage[1][2], the fees to investigate the anomalies were completely covered under their insurance policy[2]. The only cost the municipality incurred was for counsel, which fell under its retention.

Coalition[2] brings together active monitoring, incident response, and comprehensive insurance designed to mitigate cyber risk. To learn more, visit coalitioninc.com.

[1] Breach response included the engagement of an incident response firm; the insured selected Coalition Incident Response.

[2] The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.