opentext™ | Cybersecurity

Case Study

Leading Investment Firm

OpenText Network Detection & Response reduces network noise by 99.98%, accelerating effective incident response.

Replace a Legacy Tool with Scalability in Mind

This privately-owned investment firm serves more than seven million individual investors. It had long leveraged Sourcefire to detect cybersecurity threats on its large IT network. However, this provided only basic functionality and when Sourcefire was acquired, Sourcefire was eventually discontinued. A Security Analyst in the organization explains the challenge faced at that point: "Sourcefire was based on an open-source intrusion detection system and we initially turned to open source to find an alternative. After evaluating some options, it became clear that we would struggle to scale the system to cover the scope of our network traffic. We opened it up to commercial software offerings and found OpenText Network Detection & Response (NDR)."

> "At the start of our OpenText NDR journey, we had 1.2 million alerts every week, which was unmanageable. Thanks to our TAM's expert guidance on data tuning, as well as custom signature writing and deduplication processes, our security engineering team was able to reduce this to less than 200 actionable alerts."
>
> **Security Analyst**
> Leading Investment Firm

OpenText NDR is designed to examine the network from every angle with multiple detection engines to reduce noise and optimize detection. As a financial institution, there are many compliance requirements that need to be considered when evaluating potential options. OpenText NDR has a rich history with US government implementations where data security is paramount. It hosts all data on-site, without any possibility of data or metadata leakage. This was a major benefit for this client. A proof-of-concept (POC) gave the security team the opportunity to explore NDR and work closely with OpenText™ Cybersecurity consultants on initializing the systems and learning about the process of data tuning. The POC was effective in building mindshare within the team. The potential of OpenText NDR was soon clear and the decision for a permanent implementation was made.

99.98% Noise Reduction with Expert Data Tuning Guidance

OpenText NDR can be delivered as a turnkey solution, including the hardware it requires. This is optional and entirely flexible, as some clients prefer to source their own hardware, leveraging existing agreements with their hardware partner. In this case, the client

At a Glance

Industry

Finance

Location

United States

Challenge

Replace a legacy network security tool and introduce new visibility and contextual information to network security alerts

Products and Services

OpenText Network Detection & Response (NDR)

Success Highlights

- 99.98% noise reduction through expert TAM guidance
- Cost-effective data storage with data node components
- Faster and more effective incident response
- Secure onsite data hosting

> **"The combination of OpenText NDR software and our TAM helps us target our alert response in real time, enrich existing workflows, automate responses, and prevent threats."**
>
> **Security Analyst**
> Leading Investment Firm

opted for a full-service solution, including the hardware. Multiple meetings between the client and the OpenText Cybersecurity experts followed to understand the overall architecture. From this, scoping documents were produced to outline where in the infrastructure the OpenText NDR software-based sensor devices would be most effectively placed and how to size the implementation so that it would scale with the expected network growth over the coming years.

Impressed by the OpenText expertise during the POC, the client decided to invest in an OpenText Technical Account Manager (TAM). A member of the OpenText Professional Services team, the TAM serves as a subject matter expert whose role is to coach the client on the best practice of running OpenText NDR within their specific environment. This includes conducting weekly health checks and assisting with the mitigation and remediation of any software issues. With this specific client, the TAM's value really stood out when providing technical expertise to support new threat detection content.

"Within our environment, we generate a massive amount of network data and information," says the Security Analyst. "The problem is that a solution such as OpenText NDR can seem overwhelming without expert data tuning. In the beginning stages, it is important to go through an alert verification process so that our incident response teams know they can trust the information and act on it. Our TAM was invaluable in achieving this. At the start of our OpenText NDR journey, we had 1.2 million alerts every week, which was unmanageable. Thanks to our TAM's expert guidance on data tuning, as well as custom signature writing and deduplication processes, our security engineering team was able to reduce this to less than 200 actionable alerts, representing a 99.98 percent reduction in noise."

Custom signatures take known data points and match them against alerts. Today, OpenText NDR provides the contextual information to support any alert, and helps guide the responsible security analyst so that they can remediate or action an automated workflow to address the alert. This significantly boosts the incident response team's productivity and means potential security issues are identified, prioritized, and addressed much faster, with security analysts logging directly into OpenText NDR to get the full picture on any alerts.

Ongoing Knowledge Transfer and Cost-Effective Data Storage

When a new analyst recently joined the security team, the TAM proved his value once more, according to the Security Analyst: "Through on-the-job knowledge transfer, our TAM trained our new colleague on OpenText NDR and its features. Data tuning is an ongoing effort as our situation evolves continually. We are now also exploring specific customization features within OpenText NDR that will make our experience even better tailored to our environment."

OpenText NDR includes data nodes for on-site data storage. Data nodes link high-fidelity network metadata directly to events regardless of when they occur. They are flexible components that can be added to an OpenText NDR implementation when the need for more horizontal scalability arises. This gives clients the opportunity to hold a greater historical volume of metadata in a long-term repository, often required for compliance purposes. It is a cost-effective option, as it doesn't require third-party storage devices or a paid-for data lake. The OpenText NDR data storage element is a unique feature that is much appreciated by this client, who has recently expanded its data nodes by 30 percent.

The Security Analyst concludes: "The combination of OpenText NDR software and our TAM helps us target our alert response in real time, enrich existing workflows, automate responses, and prevent threats."

Connect with Us
www.opentextcybersecurity.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

768-000117-001 | O | 09/23 |