Client Outcome

10 Days to Due Diligence

Nisos Mitigates Risk for Major Retailer During Acquisition Due Diligence

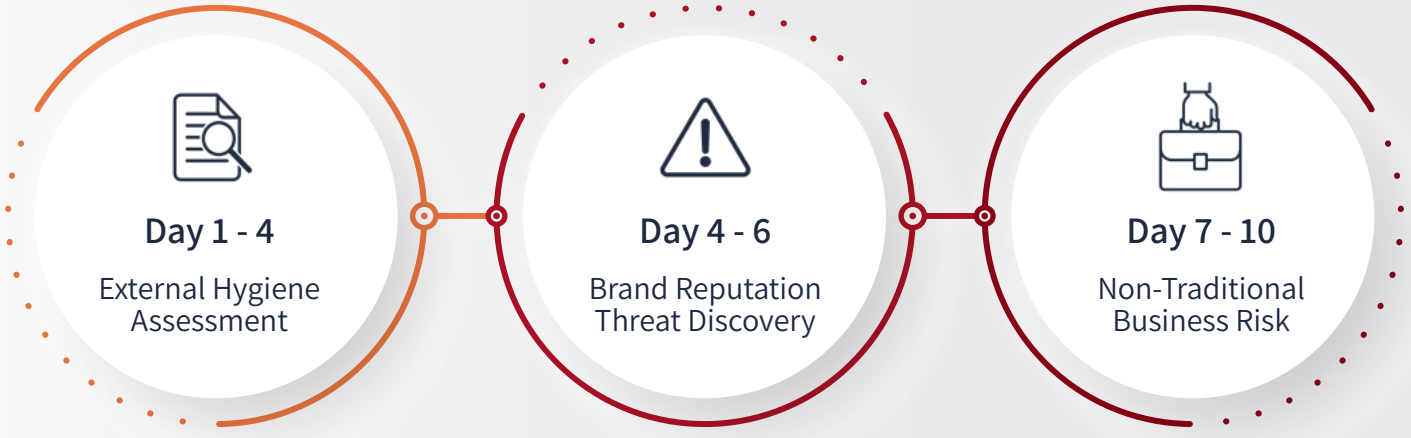
Overview

Nisos conducted an **Investment Zero Touch Diligence®** assessment for a major retailer during a period of significant growth. Our approach, using only open source data and not needing internal network access, was recognized by the client as being critical to understanding potential risks related to the internal network infrastructure and attack surface, integration, road maps, and key personnel.

The client was initially concerned about the short time frame available to perform a diligence effort. However, since internal network access was not needed and the targets of acquisition were not needing to get involved in our activities, we assured the client our process would only take 10 days.

Once our engagement began, the security and IT teams were able to leverage Nisos' assessment to validate their own findings while simultaneously conducting their own interviews to understand the targets' IT infrastructure and attack surface.

Zero Touch Diligence® Timeline



NISOS

Phase 1: External Hygiene Assessment

The client was concerned that any discovery of previously unknown cyber incidents could disqualify it from obtaining appropriate risk insurance from an underwriter. As such, counsel recommended the buyer conduct an external hygiene assessment of the target to properly assess its external cybersecurity posture.

Our Process

To begin, Nisos received external telemetry, including the domain name of the targets of acquisition.

Step 1

We mapped the target's WAN and MPLS network infrastructure and network ingress and egress points.

Step 2

We conducted external technical signature analysis using external data flows. By analyzing outbound data flows, we were able to observe multiple vulnerabilities.

Step 3

We reported our findings to the client, including a triaged list of discoveries that would directly and indirectly impact the deal.

Recommendations

Based on our findings, Nisos recommended our client examine whether the trial API was used for any customer data beyond product trials. We also recommended identifying which SolarWinds products were in use by the targets. We assessed the probability of use by Russian intelligence agencies was low due to the nature of their business and our knowledge of Russian intelligence infrastructure. We further recommended the sunsetting of old infrastructure that exposed the AWS environment to attack.

CLIENT OUTCOME: 10 DAYS TO DUE DILIGENCE

Phase 1 Key Findings

Primary Locations

Discovered primary locations associated with the targets of acquisition, including IP addresses, domains, and subdomains.

Disjointed Network Management

No centralized network management. Cloud platforms were being used for collaboration.

Transitional Tech

The target was evaluating Amazon Cloudfront. Solarwinds Orion was the current software.

Unsecured IP Address

The target's gateway IP address had ephemeral ports open to the internet for three months.

Data Leak

An API associated with a trial program for the targets' product appeared to leak data.

Exposed Data

Nisos identified 313 MB of customer data exposed on one server directly on the internet.

Outdated Software

Identification of an outdated self-hosted Python Package Index (PyPI) server. This exposed the entire AWS infrastructure to attack.

NISOS

Phase 2: Brand Reputation Threat Discovery

Similar to Phase 1, the client wanted to determine if the targets of acquisition had any mention of cyber incidents in closed forums on the internet. Following the external cyber hygiene assessment, we assessed the acquisition target's brand exposure by examining key Open Source and Dark Web data sources for reputational attacks on individuals and the company.

Step 1

We reviewed open and closed forums on the open, deep, and dark web for evidence of breached credentials, exploitable software, and direct network access offers.

Step 2

We examined the same platforms for stolen intellectual property, negative sentiment, and the presence of code in file sharing sites, such as GitHub.

Step 3

Pivoting off IP information, we utilized third parties, partners, and internal resources to identify indicators of advanced persistent threats, criminal organizations, malware, or any other threats that may have targeted the company.

Recommendations

In addition to removing outdated infrastructure, we recommended prohibiting authentication on two portals. Creating an account on one of the portals would expose sensitive client data. We also recommended the CTO ensure password variants from his Adobe account were not used in corporate or personal accounts.

CLIENT OUTCOME: 10 DAYS TO DUE DILIGENCE

Phase 2 Key Findings

Breached Credentials

Nine corporate email addresses with passwords were present in data breaches. No evidence of unauthorized access to open VPN or RDP ports was observed. No source code leaks were found on third-party repositories.

Identified Personnel

Names of numerous company employees were found in an old Linkedin data breach. The data did not appear to contain phone numbers, passwords, or other identifying information.

Closed Dark Web Forum

Actors had created an account on one of the targets' portals that could be reused on another portal. This was confirmed to Nisos investigators as an unintended vulnerability.

Vulnerability

Infrastructure associated with an old domain, including a server running a version of nginx that was vulnerable. This domain also used Zoho as its email provider, which unintentionally exposed email addresses.

NISOS

Phase 3: Non-Traditional Business Risk

In Phase 3, we assessed non-traditional business risks. We started by searching the internet for sensitive information about the acquisition target. The collection and analysis effort was similar to the steps and methodologies of the brand reputation search.

New search criteria included, but was not limited to, the presence of criminal information on executives and investors, indications of hostile control, evidence of fraud, and allegations of intellectual property theft.

Recommendations

We reported these findings, documented our sources and analysis, and recommended further inquiries for the client to pursue with the target.

Summary

Nisos Zero Touch Diligence® helped the client to be negotiation-ready with triaged, actionable findings that augmented their internal M&A analysis. We provided a comprehensive finished intelligence report that documented risk findings by type and criticality. We delivered technical data in an ingestible format for the client to use in their ongoing negotiations, ensuring risk was minimized and a desirable outcome was achieved. The client included Zero Touch Diligence reporting to validate their auditors' cyber due diligence findings, allowing them to secure the necessary insurance coverage.

Learn more about Nisos, The Managed Intelligence Company™ by visiting www.nisos.com. If you need immediate help, contact us: info@nisos.com or 703-382-8400.

CLIENT OUTCOME: 10 DAYS TO DUE DILIGENCE

Phase 3 Key Findings

Criminal Records

Criminal records for one executive. According to queries in host-country foreign media, these indiscretions occurred during his adolescence.

Organized Crime Affiliation

A previous investor had connections with organized crime discovered through a search of foreign media.

Reputation Endangerment

Geolocational and heat mapping research discovered the technology target of acquisition was located in a building with a known human rights violator.