White Paper

Zero Touch Diligence^{SM}

Extending Third Party Risk Management (TPRM) Beyond Scorecards with Actionable Intelligence

Security analysts responsible for vendor management have a unique combination of challenges, both human and technical. Questionnaires are a standard tool, but are also wrought with human error, both intentional and accidental. On the technical side, risk managers are unlikely to have access to a third party's network.

Furthermore, "on-network" investigations intended to provide appropriate cyber due diligence for third parties, such as a penetration test or compromise assessment, are rarely completed within an actionable time period aligned with the risk manager's workflow.

Finally, while risk management tools aggregate useful insights in real time, they are unlikely to be tuned perfectly to an individual risk manager's needs with a specific third party.

Zero Touch Diligence^{SM} is analyst-led, external cyber diligence that relies on a combination of automation and human investigation to provide timely and accurate insight to third-party risk management (TPRM) programs.

Zero Touch Diligence provides intuitive and actionable information that matters for businesses assessing third-party risk by fusing robust analytic methodology with a suite of tools to collect, store, enrich, and integrate data from a wide variety of sources. This facilitates tailored monitoring and professional analysis of these complex data sources, and delivers the validated, actionable results at scale to contextualize the risk to the business.

The Challenge of Security Ratings

Many security ratings companies analyze network traffic to and from an organization and other publicly accessible data sets to build security ratings for evaluating vendors and partners, pricing cyber risk insurance policies, and other use cases. The platforms also monitor so-called "hacker chatter," social networks, and public data breach feeds for indicators of compromise that had password authentication enabled for SSH connections that would allow any user with SSH privileges and the account password to login to the system regardless of having a valid key.

Additionally complicated issues for TPRM analysts include outdated information, automated and therefore unverified domain and IP lookups, applicability to the specific use case of the analyst, and the inability for automated tools to take into consideration factors such as security controls in place.

At scale (e.g., when a TPRM team has to evaluate 500+ vendors), running down false positives results can debilitate TPRM team inefficiencies and cause increased strain on the third-party vendors' infosec teams. Furthermore, depending on the size of the vendor, a security ratings tool may not include an appropriate scrub of open source intelligence (OSINT).

For example, many US companies use foreign entities for outsourced IT and security. Ratings tools are not designed to surface domestic or foreign press articles that indicate a vendor was involved in questionable legal action regarding intellectual property theft or conflicts of interest. This type of data is critical to TPRM teams to trigger appropriate follow-up and analysis to inform the business of the true risks it faces.

The Challenge of Vendor Security Questionnaires

Vendor security questionnaires have long been used as the basis for conducting third-party diligence. These succeed at satisfying regulators but do not necessarily address risk long term. The questionnaires ask a variety of questions in order to identify risks for mitigation and meet any compliance regulations.

Often, they result in checklists that either bury the lean-running vendor in questions that are irrelevant to them or result in answers that do not reflect the actual state of affairs in a larger third party. Due to the broad range of questions that often require disparate parts of a company to answer, they are often inaccurate.

Given resource constraints, TPRM analysts simply do not have the resources to review the questionnaires to accurately fact-check all of the information. They find themselves faced with a barrage of questionnaire responses that they do not have time or technical data necessary to validate, forcing the analysts to blindly trust the vendors' responses.

Analysts are forced to rely on compliance standards, such as PCI and SOC2, to prove that steps have been taken to realistically identify and mitigate risks. These compliance regimes do not indicate that a company is secure, but rather confirm the compliant party has the tools and structure in place in order to be secure in theory once risks have been identified.

Zero Touch Diligence

Zero Touch Diligence brings together cybersecurity and OSINT expertise to provide deep, current, and comprehensive insight within the proper context of an organization’s specific needs. It provides timely discovery and validation of risk that third parties could face by aggregating, enriching, and integrating data from a wide variety of sources to include:

Network and Infrastructure

Critical sources of non-public, personally identifiable information (PII)
Phone and email correlations used to provide amplifying PII to enable user attributions
Public data brokers for PII
Financial databases with company profiles
Foreign media sites, social media platforms, and limited government databases
Foreign citizen, foreign national bank, and foreign credit bank lists
Foreign flight manifest records
Geopolitical risk assessment and travel security alerts
User data from social media platforms
Mobile signals data
Global netflow data
Geolocation data, corporation associated IPs, ad-tech data graph databases
DNS, WHOIS, and threat intelligence content - including indicator of compromise (IOC) artifacts - external threats, attackers, and their related infrastructure
Monitor and query datasets containing internet facing devices (webcams, routers, servers, etc.)
Credential pairs collected from public releases of breached datasets
Deep and dark web content

Analyzing information collected from some of the same data sources on the previous page, it’s possible to understand specific vulnerabilities in the network and infrastructure of a target company. This allows us to report potential breach activity without doing a comprehensive compromise assessment or vendor questionnaire. Using global netflow analysis with mobile data, it’s possible to discover and analyze a company’s WAN and MPLS network infrastructure, the different ingress and egress points, and internal and external security products they may be using.

Further, analysis of malware infection frequency and duration of infection provides additional context to identify the efficacy of mitigation strategies. In many large companies with a global footprint, some security products may be implemented and configured differently in different areas of the world, thus increasing the risk of infection or potential infection. By reporting this information, an analyst can create a specific action plan and the company can begin to mitigate some of the vulnerabilities working with their vendor.

As always, context and analysis are important and are the primary differentiator between Zero Touch Diligence and relying on automated scoring or questionnaire technology. With the appropriate, rigorous analysis, a TPRM team can understand the real context, accurately assess risk, and apply mitigation measures appropriately.

Real-Life Application

For example, while conducting a Zero Touch Diligence assessment, we were able to uncover IP addresses directly associated with a vendor’s physical office on the public internet. This led to the identification of specific infrastructure that would likely be targeted by an advanced attacker.

Additionally, this led to the identification of a VPN server, which provided remote access to the vendor’s corporate network. We also discovered a third-party docker instance publicly accessible with default credentials. This particular instance did not belong to the vendor, but it could be leveraged by an attacker to gain control over a customer. It could also be used as an access vector leading to a potential breach of someone using the third party’s software; ultimately affecting their brand reputation and ability to generate new clients.

These discoveries are important for a TPRM analyst to use in the context of their own risk matrices. In this case, a TPRM team might only want to notify the vendor to take remediations in a given 60-90 day time window if no critical access of the third party is required. On the other hand, if the vendor requires critical access, perhaps the TPRM team might need to take more aggressive action and request indepth on-network measures like a penetration test or compromise assessment.

Deep/Dark/Surface Web for Threat Actor Activity

It is important for a TPRM team to grasp the extent of a third party's exposure on threat actor forums across the surface, deep, and dark webs. Breached credentials of key personnel, exploits for software, direct network access, or stolen intellectual property can be circulated amongst communities and forums.

Key personnel, such as senior executives or network administrators, present an elevated risk to a company. Zero Touch Diligence includes a comprehensive search of social media, surface, deep, and dark web sources for corporate and personal email addresses and selectors. Then, these selectors are used to identify credential pairs that exist amongst breach datasets or are being traded/commerced within threat actor forums.

In addition, the analysis identifies any circulating exploits regarding a third party's platforms and any intellectual property stolen and copied on text-storing and file-sharing sites like Pastebin, GitHub, Dropbox, or Mega Uploads.

Derogatory Information on Key Personnel and Investors

An often forgotten element of third party risk assessment, non-traditional business risks can be discoverable digitally. Zero Touch Diligence includes a tailored acquisition system to acquire all relevant publicly available information regarding a third party including a list of current and former C-suite executives, investors, and key figures within an information technology team. This enables investigative diligence on all relevant persons and business entities across both US and foreign press to present concise, actionable insights relevant to the TPRM team.

Examples include:

- Criminal or derogatory information on key personnel or investors
- Indications of hostile control or undue influence from criminal elements or potentially hostile nation states
- Evidence of suspicious financial activity to include insider trading or embezzlement
- Allegations of intellectual property theft, unethical practices, or whistleblower complaints

This reporting gives the TPRM analyst actionable insights that are likely to not only impact their own analysis but be boardroom-ready, if the information discovered is critical to the business as a whole.

Conclusion

Third-party questionnaires and security ratings technologies are a good starting point for TPRM teams. However, these products often lack context and validation of the information provided, which leaves critical, actionable information overlooked.

Zero Touch Diligence performed by trained cyber and OSINT investigations experts provides highly valuable and contextualized information. When used at scale, Zero Touch Diligence is capable of not only arming the TPRM team with more actionable insights but can also provide significant time and cost savings, enabling the business to act both smarter and faster to address its third-party risk profile.

For additional information, visit www.nisos.com or contact info@nisos.com.