White Paper

Full Cyber Diligence Capabilities

Can Provide Actionable Intelligence to M&A Deal Teams

Cyber Diligence

Large companies take robust consultative approaches to integrating networks and applications post-acquisition.

Rarely do acquiring security teams have the resources or cost-effective internal processes to do their own investigative cyber diligence on a pending acquisition. The most cost-effective option is intelligence analysis conducted "outside of the firewall", analysis of unique data that combines automation and human investigation to provide timely and accurate insights into key man risk, network security, negative press, and infrastructure and network vulnerabilities. Informed by this analysis, "on-network" compromise assessments can then provide a comprehensive inspection to enable the acquiring party to move forward confident it is on stable ground from a security perspective.

Challenges: Time and Focus

M&A teams are usually under tight deadlines regardless of target size, complexity, or change management process. This turnaround time can make effective cyber diligence inside the network of an acquisition difficult to complete. Sometimes, it can be unrealistic to integrate endpoint detection and response (EDR) on workstations and servers or network security monitoring (NSM) on ingress and egress points in the diligence time window.

Additionally, utilizing a third-party cybersecurity firm to integrate a cyber analyst inside the acquisition target to learn native EDR or NSM tools is often unrealistic.

Even in scenarios with more advance notice, it is rare that a security team has the time and resources necessary to dedicate requisite effort to conduct diligence on an acquisition target. The issues with vendor diligence in the context of third parties is well documented, but the sensitivity of an acquisition only amplifies third party risk issues given the timeliness of decisions that need to be made and the associated criticality to evaluate risk.

Security teams generally conduct consultative interview-based cyber diligence with the acquisition target's IT team to determine the maturity of the security stack and identify exposed vulnerabilities that could be or have been exploited by threat actors. However, depending on complexity and the size of environment, a security team may not have additional resources to get hands on the incoming network or dig in on reputation-based risks.

Zero Touch Diligence Solves for Time and Cost Issues

Zero touch diligence fuses a robust analytic methodology with a suite of tools to enrich data from a wide variety of sources.This facilitates tailored monitoring and professional analysis of an acquisition target's external-facing environment to deliver validated, actionable results, saving time and resources while contextualizing the risk to the business.

Zero touch diligence provides timely discovery and validation of actionable risk to M&A teams by aggregating, enriching, and integrating data from a wide variety of sources, including:

Values of Threats Discovered

- Non-public personally identifiable information (PII)
- 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 banklists
- Geopolitical risk assessment and travel security alerts
- Geopolitical risk assessment and travel security alerts
- User data from social media platforms
- Mobile signals data
- Geolocation data, corporation associated IP's, ad-tech data graph databases
- DNS/WHOIS and threat intelligence content including indicator of compromise (IOC) artifacts—external threats, attackers, and their related infrastructure
- Datasets containing internet facing devices (webcams, routers, servers, etc.) Credential pairs collected from public releases of breached datasets
- Deep and dark web content

Network and Infrastructure

Analyzing information collected from some of the same data sources above, it's possible to understand specific vulnerabilities in the network and infrastructure of a target company. For instance, 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.This enables reporting on possible breaches and overall network hygiene in a matter of days, without needing to touch the network.

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, inconsistencies that increase the risk of infection. As always, context and analysis are important. With zero touch diligence, an M&A team can understand the appropriate context of risk and take action to minimize it before or after its acquisition is finalized.

Deep/Dark/Surface Web for Threat Actor Activity

Zero touch diligence includes a comprehensive search of social media, surface, deep, and dark web sources for corporate and personal email addresses and data. Breached credentials of key personnel, exploits for software, direct network access, or stolen intellectual property can be circulated amongst dark web communities and forums. While there are a lot of false positives from this type of research, a robust process validates these findings through technical analysis described above to provide accurate leads for a security team to action.

Real World Application

Zero touch diligence identifies any circulating exploits regarding an acquisition target's platforms and any intellectual property stolen and copied on text storing and file sharing sites like Pastebin, GitHub, Dropbox, or Megaupload.

In one instance, a company undergoing a merger uncovered a well-developed card-skimming attack which had been present for several months. While conducting the incident response, Nisos operators identified that very early on in the breach, the attacker had posted internal source code on Pastebin. Had zero touch diligence been performed earlier, the source code could have been identified, the attacker would have been expelled, and the impact of the breach would have been significantly reduced. This discovery enabled the acquiring company to prevent "passing the breach" to its much larger environment while preserving the value of its acquisition target.

Derogatory Information on Key Personnel and Investors

Traditional diligence like interviews of executives, financial audits, and evaluation of corporate litigations often focus on easily discoverable elements of risk to validate the acquisition thesis. Zero touch diligence seeks to augment this process, using a tailored acquisition system to enable investigative diligence on all relevant persons and business entities in the US and abroad to present concise, actionable insights relevant to the M&A team. Examples include:

- Criminal or derogatory information on key personnel or investors.
- Indications of hostile control or undue influence from criminal elements or 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 M&A team actionable insights that are boardroom-ready, if critical, derogatory information discovered as well as peace of mind that extensive diligence had uncovered no information of concern.

Transitioning to the Network: Adaptable Compromise Assessments

For acquisitions that have tremendous risk in business application(s) and vulnerability, it is critical to verify malicious actors are not already resident on the target's network or applications and provide the acquiring security team valuable insights to gain efficiencies as it works to secure the new acquisition. A comprehensive compromise assessment can be an invaluable and necessary exercise.

As is the case with many acquisitions, when working with a small security team, or a hired partner such as a Managed Security Service Provider (MSSP) of the company being acquired, most actionable anomalies are identified from an event log or a signature-based alert. These alerts come from endpoint protection products, detection and response tools, or Network Security Monitoring (NSM) tools that review activity and compare it to a set of signatures or threat intelligence feeds.

If a workforce has a remote or cloud-based component, gaps in monitoring can pr esent themselves to information security teams and several variables need to be considered. In any of the below scenarios, acquiring companies should be aware of and understand the maturity of a target of acquisitions's baseline security stack (e.g. antivirus, data loss protection, OS hardening, application whitelisting, etc.). A compromise assessment will illuminate with much more granularity configurations and integrations while also determining potential malicious infections. Regardless of network size, key components of any compromise assessment to determine infection and network hygiene are visibility on endpoints, internal network, and cloud traffic.

Augmenting Signature-based Detection

Signature-based detection will identify known threats; however, adversaries go to great lengths to defeat security tools and signaturing. Seasoned actors use command and control (C2) channels and exfiltration methods that blend in with an organization's network security baseline. Identifying these sophisticated adversaries is where automated security tools fall short and Nisos excels.

Let Nisos Manage Your Intelligence

Intelligence can be a significant value-add to rapidly identify remote users infected with malware and reduce the risk of an attacker pivoting to the corporate environment. Our external data sources provide an unmatched level of visibility outside the perimeter of a corporate or home IT network, allowing us to see suspicious activity from all angles. Nisos can identify malware-infected employees prior to an attacker moving laterally into the internal corporate IT space.

Between zero touch diligence, compromise assessments andusing the proper tooling to analyze EDR, NSM, and cloud logs, organizations can gain the appropriate visibility inside and outside the networks of acquisition targets so they can ensure they are not "buying a breach". They can also gain the insights that drive actionable findings to reduce the risk of integrating the network and applications of their new acquisition in much more granular detail than general consultative interviews.

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