Deception for Mergers & Acquisitions

Mergers & Acquisitions are undertaken for a variety of business reasons to enhance, transform, and extend the business strategies and execution capabilities for organizations. The ROI of these unions are dependent on the speed of the integration and incorporation of the respective company's organizational components, operational environments, infrastructure, and technologies. The longer these activities take to complete, the higher the acquisition costs, and the longer it takes to start capitalizing on the primary objectives driving the union.

Combining technological infrastructures can create significant complexities in the form of integration challenges, technology overlap, misalignment in fundamental processes, technological disparity, and diverged maturity. The speed and accuracy of an organization's due diligence and assessment of these integration elements is fundamental to enabling the most efficient strategy and plans for integration. Notably, despite this due diligence, 40% of acquirers reported discovering a cybersecurity problem after a deal completed .

When an acquisition is announced, both organizations experience an increase in target profiles and public visibility. This typically results in both organizations making themselves targets of increased cyber threats and attacks. In Testing the Defenses: Cybersecurity Due Diligence in M&A, West Monroe Partners reported that,

In the realm of M&A, concerns about cyber security are becoming a critical issue when companies target acquisitions. A company's cyber security infrastructure—or lack thereof—can affect the deal price, and at times determine whether a potential acquirer goes through with a deal at all

With the threat landscape that exists today, both organizations must assess the security integrity, maturity, and current state of the newly acquired entity's network and infrastructure. This drives the need for technological approaches to rapidly establish visibility and the means to ascertain the risks and vulnerabilities that may exist related to:

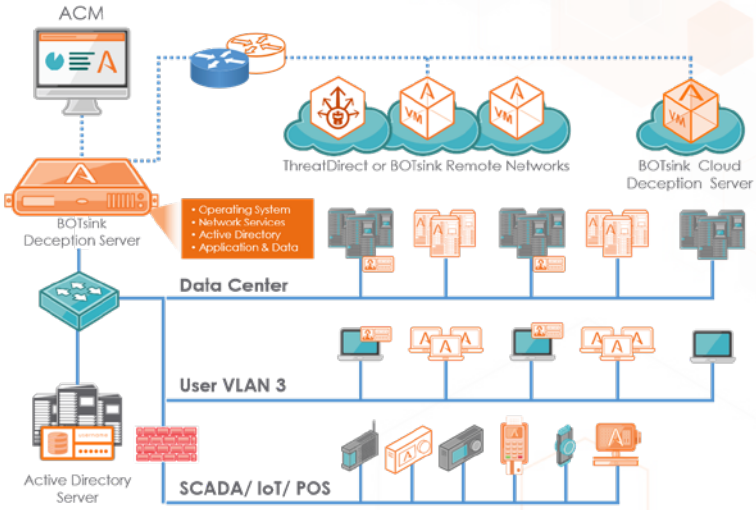
- The state of current security controls and processes
- Identifying potentially active compromises and vulnerabilities that may exist
- Gathering intelligence and understanding the current infrastructure across cloud, data center, end user networks, and even into operational networks like SCADA/ICS/IoT/ POS networks.

All of these discovery elements can be used as due diligence to develop a strategy to address and identified deficiencies, aid in reducing risks, and elevate the security posture of an environment. An effective assessment and the development of a remediation plan ensure that the technological integration doesn't result in 'poisoning the well' and that the acquisition initiatives aren't jeopardized or impeded.

The Attivo Networks® ThreatDefend™ Deception and Response Platform is designed for high-interaction, deception-based threat detection that is delivered through a network of distributed decoys to deceive, detect, and defend against human and automated attackers including Advanced Persistent Threats (APT), credential thefts, BOTs, insider threats, malware, ransomware, phishing attacks, and more. Once deployed, the platform provides insight and understanding into threats in the network, aiding the discovery effort and providing visibility into the risk of a breach.

Network Threat Visibility & Detection

The ThreatDefend solution helps establish network visibility and aids in understanding the threat risk within the new network environment. The solution will not only identify any active lateral movement that could be occurring but also learns and understands the resources in the networks involved, and presents this through powerful visualization maps. Deploying the Attivo solution will identify active in-network compromises, vulnerabilities, and threats that may already be present in the new environment. The Attivo solution is non-intrusive as it is not inline and does not require endpoint agents to operate. Deception can be deployed within a day and provides rapid visibility, detection, and accelerated assessment insights.



Attivo has a successful track record for delivering this visibility and assessment capability to retail and other industries, as, for example, post-acquisition discovery in conjunction with integration efforts prior to a formal acquisition announcement. The latter use case enabled the organization to identify security risks and vulnerabilities that needed to be addressed and remediated before the formal acquisition announcement was made.

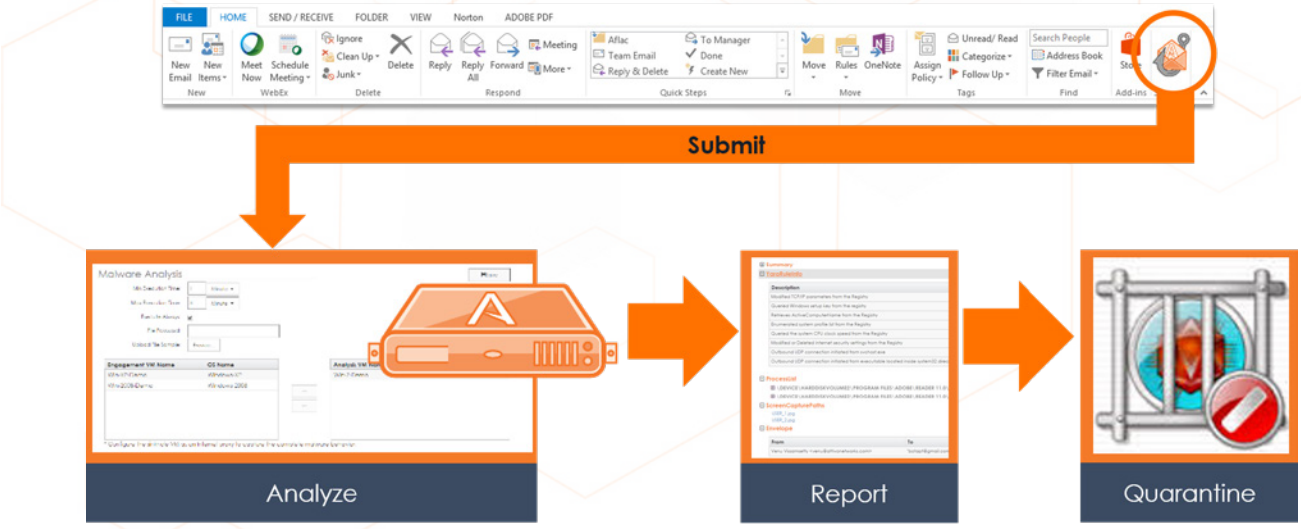
How Deception Technology Works

Organizations gain visibility by creating and deploying engagement servers (decoys) within datacenters, end user networks, cloud infrastructure, and specialized environments like SCADA, ICS, IoT, POS, SWIFT, or telecommunications. Deception credentials, lures, and objects can also be applied at endpoints and Active Directory servers for detection of credential harvesting. The decoys are projected into the environment, designed to detect lateral movement based on engagement, and positioned to identify risks associated with East-West traffic. The deception engagement servers collect information from adjacent systems through passive observation of network traffic, including host names, OS, Mac addresses, services, traffic, and protocols. The Attivo system then builds a visual map of those production resources, decoys, and its deceptive engagement servers, providing valuable data that facilitates comprehensive and expedited assessment efforts. Network visualization maps can also show time-lapsed changes to the network environment. The addition of deception technology in a network can be instrumental in identifying not only potential attacks on the network, but also misconfigurations and exposed credentials that create risk for attacker entry and attack escalation.

Identifying and Understanding Active Compromises

Any active compromises, credential harvesting, Man-in-the-Middle, malware, ransomware, APTs, reconnaissance, and insider threats, that may be in the environment will be detected based on interaction, the use of lures, and engagement with any Attivo deceptive decoys. The solution integrates with Active Directory to detect Active Directory queries within managed networks, and can also identify misconfigurations that allow an attacker to leverage stored or orphaned credentials on endpoints within the network to laterally propagate. The ThreatDefend Platform includes an attack threat analysis engine (ATA) that provides attack correlation and full forensic-based threat reporting for all activity that occurs in the deception environment. The ATA will identify full threat TTPs, including payload drops, registry changes, identified malware propagation methods, and SHA-1 signatures. Detailed forensic products provide significant value in addressing and identifying broader vulnerabilities in the environment that may need to be addressed.

The Malware Analysis Sandbox (MAS) is a decoy converted into a dedicated binary analysis VM that will analyze any suspicious executables from phishing emails, potential malware, and other threats to capture lateral movement methods, observe malware behavior, and identify attacker IP addresses such as Command and Control IPs on the Internet. The Attivo architecture is built on a full OS environment, enabling high-interaction decoys and the ability to collect comprehensive attack analysis. Within this safe sandbox environment, exploits can fully develop without time constraints, and can be instrumental in understanding and shutting down polymorphic attacks. The MAS will identify full threat activity, including payload drops, registry changes, malware propagation methods, and SHA-1 signatures. Detailed forensic products provide significant value in addressing and identifying broader vulnerabilities in the environment that may need to be addressed.



Through 3rd party integrations (Firewall, SIEM, NAC, Endpoint), the platform can automatically share attack information with existing security controls to accelerate the blocking, quarantine, threat hunting, and remediation of vulnerabilities. Organizations using the Attivo ThreatOps™ solution can also create repeatable playbooks based on their security handling process and the profiles of an attack.

Central Management & Distributed Location Coverage

If multiple BOTsink solutions (hardware, cloud, or virtual appliances) are deployed across multiple data centers, satellite offices, or operational locations, the Attivo Central Manager (ACM) provides quick and effective management and aggregation of threat information across the distributed production environments. The ACM can be deployed in an on-premises capacity or in AWS, Azure, or OpenStack today.

Additionally, Attivo provides a lightweight forwarder VM, called ThreatDirect™, which can be deployed into remote offices and locations where a dedicated appliance is not viable, giving visibility to threats within those locations. This same technology can also be applied in micro-segmented networks.

The BOTsink engagement server can also be useful in identifying Darknet threats through dynamic engagement, redirecting, or terminating traffic from a machine that is scanning unused IP addresses.

Credential Attack Path Lateral Movement Identification

The ThreatPath™ solution includes the ability to analyze endpoints for misconfigured, exposed, or orphaned credentials, which helps to proactively identify lateral movement paths that may provide an available attack path. Identifying these vulnerabilities enables security teams to remediate them before attackers can make use of them. Integrations with service workflow providers like Service Now and Jira will be available in the second half of 2017.

Conclusion

The Attivo Networks ThreatDefend platform has a proven track record in playing a crucial role during M&A due diligence and post-acquisition integration. By detecting hidden threats, identifying security deficiencies, and providing risk visibility, these insights can be applied to mitigate risk and to strengthen the combined organization's overall security posture. The platform can instantly detect and alert on suspicious behavior that may arise from new network access including insiders, suppliers, and contractors, and will provide detailed forensics to understand and quickly react/respond to anomalous behavior. Many detection solutions take time to tune and "get good" before they can provide detection value. The Attivo deception technology platform begins working immediately, and provides timely visibility, detection, and the attack information required to understand the health and resiliency of a network and shut down threats before attackers have time to complete their mission.

About Attivo Networks

Attivo Networks® is the leader in deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber attacks. The Attivo ThreatDefend™ Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. Attivo Camouflage dynamic deception techniques and decoys set high-interaction traps to efficiently lure attackers into revealing themselves. Advanced attack analysis and lateral movement tracking are auto-correlated for evidence-based alerts, forensic reporting, and automatic blocking and quarantine of attacks. For more information visit www.attivonetworks.com