Going on the Offensive with ThreatDefend™ Attack Intelligence

Threat Intelligence, Adversary Intelligence, and Counterintelligence

As a rule, would you consider your security team a defense or offense-based organization, or somewhere in-between? An offensive team would favor bold pre-emptive measures, whereas a defensive team is more likely to build fortresses and wait and react. Any good security plan must be able to do both as the situation warrants, factoring in that each organization will have their own style and tendency to favor one over the other based on their available information, program maturity, and ability to apply advanced security strategies.

Attackers have traditionally had the offensive advantages of subterfuge, stealth, and surprise in cyber incidents. They leverage many techniques to remain hidden and “under the radar” while network defenders deal with manpower shortages, information and alert overload, an ever-expanding attack surface, and many other challenges. To address this imbalance, information security teams are turning to deception to change the asymmetry in cyberwarfare against attackers. The Attivo Networks ThreatDefend Deception and Response Platform is ideally suited to detecting attackers that have infiltrated past perimeter security and are in the network. The ThreatDefend platform’s network and endpoint decoys, breadcrumbs, and lures work to mislead attackers, diverting attention and attacks to deceptive assets that alert and record all their activity. This information is then applied to gain insight into all facets of the attack and for obtaining rich threat intelligence, adversary intelligence, and counterintelligence. With this level of information organizations no longer sit in wait for the attacker to make a blatant mistake or for a 3rd party to send notification of a breach. Instead, they can apply this intelligence for faster response and remediation, and for proactively understanding attacks, enabling them to better understand an attacker’s mission and fortify their defenses.

Threat Intelligence

Indicators of Compromise (IOCs) are the most common product of threat intelligence collection and development. Upon attacker engagement, the ThreatDefend Platform captures all attack activity and provides information and metadata on attack tools, IP addresses, network traffic, and many other facets of the attack. These IOCs provide information that security teams can use to identify potential victims or strengthen existing defenses. The ThreatDefend Platform’s use of full operating system decoys enables the highest levels of authenticity and interactivity, deceiving attackers into believing they are interacting with a production system instead of a decoy. This allows the attacker to explore the decoy as deeply as they wish while unknowingly providing the security team with extensive threat intelligence.

Adversary Intelligence

Security teams seeking to understand the attacker will look to identify and analyze their Tactics, Techniques, and Procedures (TTPs), patterns of activities or methods associated with a specific threat actor or group of threat actors that identify HOW attackers are attacking. The ThreatDefend Platform provides insight into TTPs by capturing all aspects of attacks from start to finish, giving security analysist data they need to develop adversary intelligence, helping with risk management and incident response. This includes being able to capture advanced interactions such as opening communications to command and control to capture time-triggered and polymorphic actions.

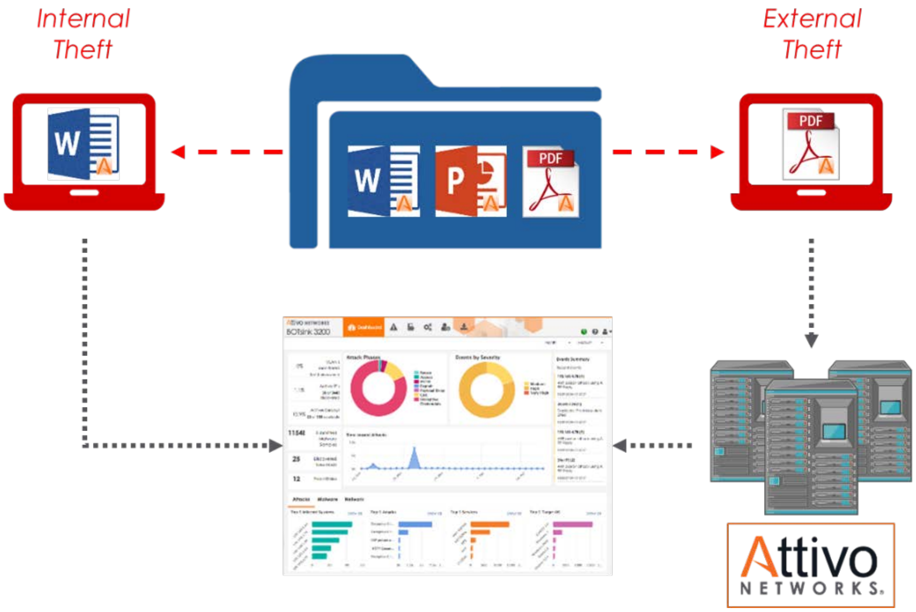
Counterintelligence

The ThreatDefend Deception and Response Platform provides an inherently offensive counterintelligence function. The solution seeks to disrupt and degrade the information-gathering and attack operations an adversary conducts inside the network, while at the same time providing collective counterintelligence functions by helping develop threat and adversary intelligence.

While IOCs and TTPs help security teams answer how attackers are attacking, there remains the difficult task of identifying WHO is attacking while gaining insight into what information they are seeking to steal. The ThreatDefend Platform's DecoyDocs solutions provides the ability to plant deception files that allow the organization to track documents that were exfiltrated. By embedding a tracking call-back function into a document, the DecoyDocs solution can provide data on what was stolen and beaconing to identify where an attacker opened the file. The DecoyDocs callback provides the externally facing IP address and geolocation of every system that opens the DecoyDoc and the name of the file stolen thereby providing data that can help with attribution, identification, and proactive security measures.

DecoyDocs are fast and easy to set up. Word, PowerPoint or PDF files are loaded into the BOTsink engagement servers where they are tagged for tracking and a notification email address set up. The Attivo Networks cloud security service will then alert via this email address any DecoyDoc notices arising from beaconing alerts.

Today's modern attacker is making fewer and fewer mistakes, making a reactive defense less and less effective. By gathering early and detailed threat-, adversary-, and counter-intelligence organizations can take a proactive posture to their organization's security and ultimately call checkmate on the attacker.



DecoyDocs create an alert when opened inside or outside of the network

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www. attivonetworks. com