Stratecast | FROST & SULLIVAN

July 29, 2016

Deception as a Security Discipline

Going on the Offensive in the Cybersecurity Battlefield

Stratecast Analysis by

Michael P. Suby

Stratecast Perspectives & Insight for Executives (SPIE)

Volume 16, Number 27

Deception as a Security Discipline
Going on the Offensive in the Cybersecurity Battlefield

Introduction[1]

Security analysts tasked with overseeing alert investigations and incident response are inundated with security alerts. The origination of alerts is far from singular in nature as they arise from both internal operations and cyber attackers. In internal operations, the combination of IT hybridization (on-premises and cloud), end users with multiple devices, the Internet of Things, and partner and supplier integrations, contributes to a complex and broadening system of assets, connected devices, and interrelationships. Moreover, this system morass is dynamic. It changes constantly, for a number of legitimate reasons such as revised business requirements, altered circumstances, and the introduction of new applications and technologies. And with change representing deviations from the norm, even if anticipated, the alert pile can still increase in size.

The user community also represents its own slice of uncertainty and non-conformity. In the spirit of attending to business, users veer from their normal routines, and they also cross the boundaries of acceptable practices (e.g., sharing and reusing credentials, and sharing other forms of sensitive information with individuals that are not in the "need to know"). Additionally, they unintentionally, but nevertheless directly, place the business at risk by providing a toehold for malware in internal systems through divulging their credentials when, for example, they are tricked into clicking on dubious email attachments and interacting with questionable Web sites. All combined, operations and user activities add to alert volume.

Cyber-attacks, the core focus of security analysts, are the ever-present wild card and a prominent cause for alert generation. Professional attackers, however, are fully aware that deviation-tripping alerts call attention to their activities and potentially put a stop to them. Therefore, they pattern their activities to minimize detection (e.g., proceed slowly) and cozy up to routine operational behaviors. Even when their activities generate alerts, dressed the same as the crowd of operational- and user- triggered alerts, attackers gain time in the pursuit of their ultimate goal—exfiltrating valuable data.

> ***For security analysts, a high volume of alerts, attackers' activities spread over a lengthy period of time, and undifferentiated alerts challenge their effectiveness and speed to detect and respond.***

For security analysts, a high volume of alerts, attackers' activities spread over a lengthy period of time, and undifferentiated alerts challenge their effectiveness and speed to detect and respond. The casualties to the business are, unfortunately, many, and worse, on-going. Most damaging is the exfiltration of valuable data long after the attacker first circumvented perimeter defenses and landed in the inside. From a post-breach

[1] In preparing this report, Stratecast conducted interviews with representatives of the following companies:

- Attivo Networks – Marc Feghali, Co-founder & VP of Product Management; and Carolyn Crandall, CMO
- ForeScout Technologies – Marty Davis, Senior Director of Business Development and Alliances; and Sandeep Kumar, Director of Product Marketing
- Blue Coat Systems – Peter Doggart, Vice President of Business Development

Please note that the insights and opinions expressed in this assessment are those of Stratecast, and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

forensics perspective, a comprehensive mapping of the attacker's intra-system movements may not even be possible, as the attacker's first landing point and reconnaissance activities may not have caught attention and been recorded. Consequently, the means to remediate all points of vulnerability that allowed the attacker to succeed, and to improve alert handling and incident response, is restrained. Sadly, the attacker's ability to strike again in the same manner has not been completely vanquished.

These circumstances are not new. A variety of security tools are used to improve detection of attacker infiltrations, and speed alert investigations and incident response. User behavioral analysis (UBA) and security information and event management (SIEM) are two such tools that leverage a far-reaching range of system and device logs, and triangulate with a variety of external threat intelligence sources to identify and confirm indicators that an attacker is inside, which assets have been touched, and map the sequence of attacker movements.[2] As valuable as these security solutions are, they extensively rely on identifying bad actors' activities relative to legitimate behavioral baselines, which is mixed in with the clutter of baseline deviations originating from changes in operations and user activities. As a result, valuable time and security analyst talent are consumed in wading through the clutter to ascertain bona fide, high-risk alerts that bear priority handling.

Might there be a means to consistently produce high-fidelity alerts that are unmistakably associated with attackers and malicious insiders, which include a comprehensive catalog of the attacker's system moments, and are triggered in real-time? That, in a nutshell, is the objective of deception, and the focus of this week's insight. Also included in this insight is a brief description of a deception solution provider that has been making headway in this new security category—Attivo Networks.

The Basics of Modern-Day Security Deception

In reality, the idea of keeping attackers completely out of the network is fundamentally flawed. As human error is, by nature, prone to occur, and attackers will continue to get more sophisticated and targeted in their tactics, even the "castle with the tallest walls and largest moats" can be penetrated. **A different approach is needed; one that has been used for decades to beat attackers at their own game.** Rather than watching every movement and action on the network, and correlating with "known good" behaviors to assess maliciousness, set traps that mimic the attackers' targets, and lay bait to lure the attackers into these "no way out" traps. **At its core, deception, as this approach is called, is about tricking a foe into engaging and revealing itself—the antithesis of the foe's intent—and without the foe realizing that it has been discovered.**

This task is not simple, as modern-day attackers are "grade-A" students of past and present security technologies. They will scale great heights to thoroughly understand security technologies and the operational IQ, and practices of the organization's security team; to identify weaknesses, and exploit those weaknesses so they can continue to succeed in locating and extracting valuable data.

Deception adheres to the same precept as attackers: understand the adversaries' motivations and associated practices, in order to exploit their vulnerabilities.

Deception adheres to the same precept as attackers: understand the adversaries' motivations and associated practices, in order to exploit their vulnerabilities. **Deception, by design, turns the tables from being the hunted to being the hunter.** Broadly

[2] In-depth analysis on the driving forces behind the double-digit market growth in SIEM is contained in *Analysis of the Global Security Incident & Event Management (SIEM) and Log Management Market – All Information Becomes Actionable*.

speaking, there are three types of attacker motivations and associated practices, described below, which form the basis for deception's exploitation of attackers' vulnerabilities:

- **Information is attackers' currency** – Attackers' success depends on information about the hosts and systems they invade. With cunningness and persistence in gathering host and system information (e.g., credentials, browser history, cookies, and VPN configuration files), attackers have demonstrated that they can gather enough information to map out pathways to valuable data, and then extract that data. Feeding attackers' thirst for information can be turned into an ally in deception and redirecting attackers away from valuable assets.

- **Initial reconnaissance steps are the attacker's most vulnerable** – Upon invading a system host, the attacker takes its initial steps to gathering system information—that is, conducting reconnaissance. Since these initial steps occur when the attacker knows the least about hosts and the system (a foreigner in a new land), the attacker's ability to disguise its reconnaissance activities, and discern real and useful versus fake or unimportant system information, is at its weakest. Seizing on this state of attacker vulnerability, deception broadly paints the hosts and the system floor with sticky breadcrumbs, per se, to indelibly mark the attacker.

- **Return on investment** – Attackers vary in resources and financial backing. Although prolonged attack planning may not add material expense to an attacker, as some of the planning can be applied to multiple targets, deception techniques employed in a target's network can effectively drain the attacker's available time and resources by deceptively engaging the attacker as it escalates its attack. Once the attacker realizes that meeting its objectives with a deception-guarded target will not occur within the attacker's parameters of time and resources, the likelihood of the attack being abandoned increases. **At a minimum, with a deception minefield, the attack becomes more complex; and, ideally, the attacker re-aims its sights on targets that are faster and easier to exploit.**

With these attacker vulnerabilities in mind, the following is a generalized three-step description on how deception operates:

- **Spread the bait and set the trap** – Attractive but fake host and system information is planted strategically throughout the system. Much like the legitimate host and system information that attackers gather to build a pathway to valuable data, this fake information builds a pathway to an artificial or decoy environment (the trap) that is off the production system and network, and away from real assets.

- **Attackers take the bait** – Attackers pick up this fake information during reconnaissance, and are lured to the decoy. With the fake information disassociated with real system information, the collection of this information marks the attacker; that is, only the attacker will have this information, and only the attacker will be lured into the trap. Correspondingly, this creates a high-fidelity indicator.

- **Attackers are captured** – Once directed into the decoy, the attacker is now unknowingly captured. From this point forward, the attacker's actions are observed without placing real assets at risk. In fact, the reverse happens: risk can be reduced. The attacker's observed actions, which are unmistakably associated with the attacker, arm security analysts with high-confidence information on compromised hosts, system vulnerabilities, external command and control servers, and other forms of dangerous destinations.

Deception Solution Attributes

Deception, as previously described, is finding a renaissance (in the context of honeypots that have been in use for many years) as a security solution category. As such, the market is dominated by entrepreneurial companies aiming to demonstrate long-term customer value, and to be among the leaders when the market consolidates. Correspondingly, sustainable differentiation and speed-to-market are trajectories that deception vendors are pursuing. Nevertheless, we believe there are four essential and correlated solution attributes that both enterprises and technology integration partners should consider as they kick the tires on deception. **The four attributes for evaluating deception technology are: authenticity, vitality, automation, and ambition.**

- **Authenticity** – Wily attackers are not casual bystanders. They are directing a serious business: the business of stealing valuable data, and profiting by the use and resale of these stolen goods. Upon realization that deception solutions are making their way into an enterprise's security fabric (if not already), attackers will direct their development efforts on countermeasures—detecting when deception is on-board in their targets' systems, and devising means to offset its effectiveness.

  Simulating the enterprise's genuine portfolio of hosts and system design in breadcrumbs and decoys is, therefore, essential. But practicalities enter in. The extreme scenario of full duplication would be cost prohibitive and conceptually unjustifiable—why create fake instances of everything when a façade would be just as effective? So, in practice, the deception solutions need a strategy for determining optimal density and variety of breadcrumbs and decoys. This, in turn, raises the question of how to measure effectiveness. For that, our recommendation is to understand how closely the decoys and deception lures match the production environment. **Effective deception includes a comprehensive set of deception lures with personality credential matching, validated against the organization's user directories (e.g., Microsoft Active Directory), and that are dynamically updated to circumvent attacker detection. Also, the decoys are easily configurable to reflect the real operating systems and golden images of the production environment.**

- **Vitality** – Enterprise systems are, metaphorically, living and breathing organisms; they are constantly changing. Moreover, if the target is attractive enough or the means to launch an attack is low enough, the attacker is likely to revisit the same target, if for no other reason than to exploit a new vulnerability. In order to be believable, the deception must adapt: that is, demonstrate vitality. If, for example, the attacker determines no change in its reconnaissance efforts (what is returned from deception), the attacker could conclude that deception was used and that the deception tactics have grown stale; that is, they no longer accurately reflect the system's current configuration. In turn, the attacker may pursue a different approach to reach its objective. In a sense, vitality is related to authenticity. The deception must align with the current reality; an authentic representation of the hosts and system at a point in time is insufficient. For example, if the organization uses a mix of Windows XP and 10 in production, a deception that only includes Windows XP may be detectable by an attacker. Also, part of vitality is staying current with trending attack methods that include an element of "once inside," such as advanced persistent threats (APTs). To that end, the deception solution should have a demonstrable track record of developing effective mitigation for new and updated "once inside" attack methods.

Advanced deception solutions do not require manual intervention, and are equipped with self-learning deception credential deployment in which the deception system uses environmental learning to automate the deployment and updating of credentials.

- **Automation** – Good security technology becomes a weak security practice if the effort to manage and maintain is onerous. This same sentiment applies to deception. In consideration of the previous two attributes of authenticity and vitality, an overly manual effort or expertise requirements in the ways of deception will contribute to the downfall of effective deception. How much effort or required expertise is more than acceptable is, however, an individual company assessment. Proof of concepts assist in gauging how much of each is to be expected when the deception solution is fully operationalized. If the deception vendor designed its solution with ease-of-use automation in continuous threat management, there is reason to be optimistic that the promise of effective deception will be realized.

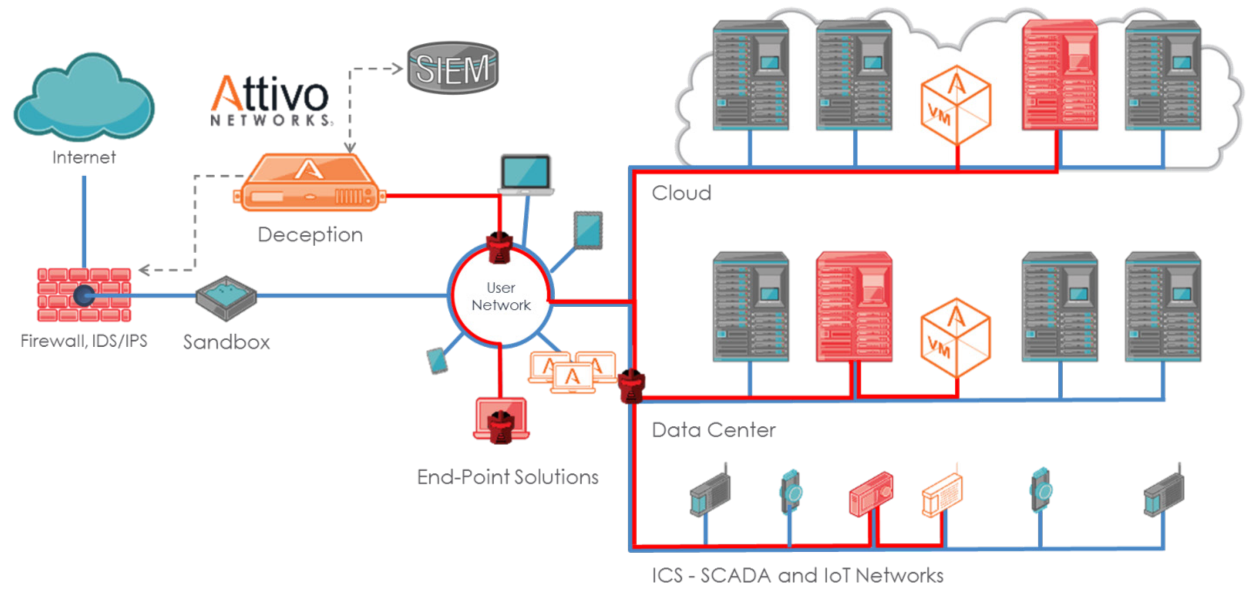
  As a backdrop, security operations teams spend valuable time correlating attack data to assess threat severity; and gathering and evaluating forensic data to stop and remediate attacks. An effective measurement of deception's value compares the number and quality of incremental alerts that are generated through deception, in relation to the current alert-generating processes and, equally important, the fidelity of these alerts (i.e., are there false positives?). Another measurement is the time saved in having the entire attack lifecycle systematically gathered; and trusted incident response actions automatically fed into prevention systems, to stop attackers and instantly quarantine infected systems from the network. **At a time of perpetual IT and security staff shortages, deception provides much-needed accuracy and efficiency in attack detection and remediation.**

- **Ambition** – Identifying and undermining attackers that have reached the inside of an enterprise's network, with a high degree of certainty—while a major and valuable accomplishment of deception—is another point of confirmation that security, in general, is broken. Deception as a security solution exists because preventive measures, such as perimeter defenses, were only partially effective in keeping the bad guys out. Also, there is no guarantee that all attackers that crossed the perimeter will be found and their exploits stopped before real harm has occurred. The reality is that there are, unfortunately, no absolute guarantees in security. Therefore, deception as a security category, like other security categories, must continuously strive to deliver more value (i.e., do more, be better). Essentially, deception solutions should have ambition. For example, deception solutions should not be islands of functionality. There should be cross-security technology integrations to further strengthen threat analysis and accelerate incident response. Ultimately, deception solutions should also play a role in enterprises becoming more proactive in risk management; that is, anticipating and circumventing attackers' next moves. If deception can provide definitive statements on attackers' current practices and behaviors, that intelligence should also be mined to predict and circumvent what they will likely do next.

Attivo Networks

Founded in 2011, **Attivo Networks exemplifies a modern-day approach to deception.** The company begins with the premise that attackers will, if they have not already, reach the inside of the enterprise's network. To uncover attacker existence and render them ineffective, Attivo designed its solution to be system agnostic. Like its customers' networks, Attivo supports a mix of subnets and hybrid compute locations, so the breadcrumbs can be placed in a wide variety of system environments—e.g., user devices, networks, clouds, private data centers, industrial control systems (ICS), and Internet of Things (IOT). This system-agnostic approach is displayed in the illustration of the Attivo ThreatMatrix Platform in Figure 1.

Figure 1 - Attivo Networks ThreatMatrix Platform



Source: Attivo Networks

With the Attivo ThreatMatrix Platform, the breadcrumbs are inserted in all desktops and servers; and the orange colored devices, which can be virtual machines (VMs) or appliances, sit alongside real devices and VMs in each of the four system environments. While the attackers (the red and black helmet icons) can "see" these artificial devices, and scoop up the breadcrumbs (e.g., fake credentials and a variety of attractive but fake network, system, and application information) as they move laterally from an infected host (red device icons), these Attivo-planted devices and VMs are invisible to legitimate system users and operations.

The spreading of breadcrumbs causes no disruption or alteration to existing systems or operations; it is a transparent co-existence. The breadcrumbs, as previously described, mark attackers and lure them to an interactive Attivo ThreatMatrix BOTsink deception server (the trap), and can be located either within or off of the production networks (depicted as the orange "Deception" device icon). Designed to mimic real systems, the ThreatMatrix BOTsink deception server, in collaboration with the Attivo Multi-Correlation Detection Engine, is a safe environment for observing and analyzing attacker IP addresses, methods and activities.

This attacker intelligence is viewable in the Attivo Threat Intelligence Dashboard. This same intelligence can also be exported into SIEMs, and can generate indicators of compromise (IOC) and structured threat information eXpressions (STIX), to assist in threat hunting, and fed into prevention systems for incident response (e.g., blocking, isolation, and device remediation).

Four Attribute Assessment

In this section we assess Attivo Networks alignment with the four solution attributes we previously described: Authenticity, Vitality, Automation, and Ambition.

Authenticity

In creating a believable deception tailored to an organization's unique system circumstances and assets to protect, the Attivo ThreatMatrix Platform supports deception-building capabilities across a wide range of virtual machine types (Windows, Red Hat, CentOS, and Ubuntu); end-user devices, system and network services and protocols (e.g., Active Directory, NetBIOS, HTTP/HTTPS, and MySQL); supervisory/process control devices, protocols and standards commonly used in supervisory control and data acquisition (SCADA), and Internet of Things (IoT) systems; and credentials.

Credentials are particularly noteworthy, as they are: (1) highly attractive to attackers, as they are the access keys to valuable assets; (2) diverse in type and operating system; (3) numerous; and (4) unique to each organization. In addition to providing extensive support for credential type (e.g., credential hashes, browser, CIFS shares, email client, and FTP client) and operating system (Windows, Mac, and Linux), Attivo offers wizards, administrative tools, and directory integrations to help its customers in creating and updating deception credentials: based on the organization's policies on refresh intervals and configurations, geographic footprint, and even quantity. Attivo also guides its customers on subtle but reusable deception ploys, such as recycling the credentials of recently departed employees, as deception bait. Recently, Attivo added self-learning to personalize credential deployment; and now also offers automated credential deployment and refresh.

Vitality

Recurring reconnaissance is also employed by Attivo, not for exploitation purposes as with attackers, but to produce a heat map of the organization's systems to determine where and what breadcrumbs to put in place, and the dimensions of the deception environment hosted in the ThreatMatrix BOTsink deception server. From a continuity perspective, as an entirely software-based platform, changes to the production system and devices can be reflected in the end-to-end deception environment, bait and trap, on a near-continuous basis. In this manner, an evergreen deception environment is ensured.

With regard to adapting to the evolution in attacker methods, the ThreatMatrix platform has purpose-built mechanisms to mitigate email phishing attacks, and file encrypting ransomware. To identify and mitigate email phishing attacks, questionable emails with their file attachments are sent by users to the ThreatMatrix BOTsink deception server, where the email and its attachments are activated in this controlled environment (a replication of the organization's production system), to assess intent. Included in this assessment are extensive details on network connections attempted, registries accessed, and process and file activities. Screenshot images of the email execution are also captured, so organizations can make an informed decision on next steps—such as automatically quarantining the email message.

Since the end-to-end process is occurring in real-time, and the user involvement is limited to pressing a "click to send" icon in the email client (enabled by an email client plugin), disruption to the user is very slight. Moreover, with slight user impact, this mechanism has the potential to promote greater vigilance by users in their email discretion; that is, when there is even the slightest concern on email message reputation, "click to check" before "click to read."

The mechanism for identifying the existence of file encrypting ransomware, so its propagation can be contained, differs slightly from the email phishing mechanism. Rather than triggered by users sending questionable emails, the ransomware—as it moves laterally to encrypt more local user files and the more coveted network drives—is lured into the BOTsink deception server, where analysis is conducted as the ransomware encrypts documents in the BOTsink network drives (fake documents in fake network drives). Supported with clear evidence on the existence of ransomware and its code, the organization can confidently initiate steps to contain the spread, such as quarantining the infected subnet; and remediate infected devices by first conducting a targeted scan for the ransomware.

Automation

In the previous two attributes, features of the ThreatMatrix Platform that cross over into this Automation attribute were noted. They include establishing and maintaining deception realism, and automated mechanisms to fight advanced threats, man-in-the-middle, credential, phishing, and ransomware attacks. Also, pertaining to automating deception realism, Attivo customers can upload golden images of their end-user devices and services into BOTsink; a time savings over manual creation.

The Attivo ThreatMatrix Deception Platform is also designed for efficiency, and is dramatically different from earlier generation honeypots. Attivo has made significant advancements in deception techniques by simplifying deployment and operations, supporting self-healing attack environments, and offering stealth mode deployments to avoid interference with other network scanning devices. Deception pervasiveness is also essential. Recognizing that attackers view branch offices as soft targets, Attivo recently extended its deception capabilities into branch offices. By integrating centrally-managed decoy VMs into the business's existing branch network routing infrastructure, Attivo inserts the same intensity of deception effectiveness into branch offices as in headquarters locations; and with the operational scalability and remote administration that branch office deployments demand.

Of high importance for security analysts is the ability to seamlessly work across multi-vendor, multi-technology security infrastructure to support operations—namely, detection forensics and incident response. This, too, is an Attivo ThreatMatrix Platform feature, and a feature that crosses over into the next solution attribute: Ambition.

Over the last year, Attivo has established technology integrations with multiple security vendors in detection forensics (SIEM) and incident response (perimeter defenses). Two partners were interviewed in preparing this insight: Blue Coat Systems and ForeScout Technologies. **A common interest shared by Attivo integration partners is the improvement their customers gain in mitigating risk with greater confidence by incorporating ThreatMatrix high-fidelity alerts into automated and semi-automated incident response policies (e.g., block, quarantine, and remediate).**

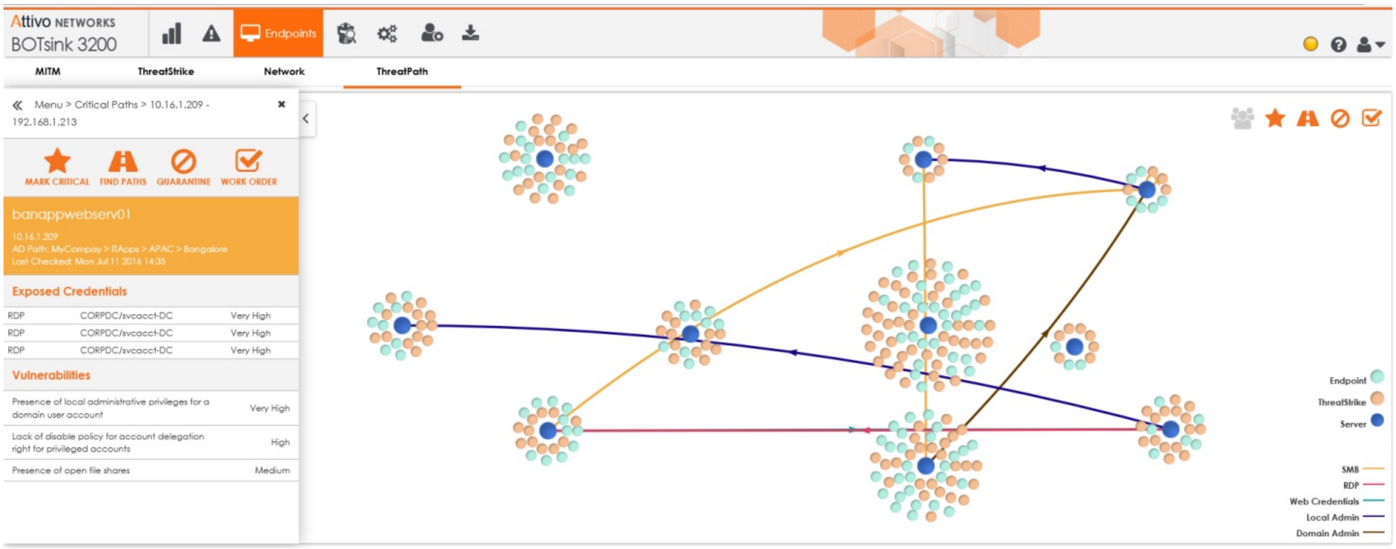
On SIEM integrations, ThreatMatrix high-fidelity alerts and detailed IOC are automatically fed into SIEM forensic engines. Combined with the SIEM's other IOC sources, vulnerability knowledge, client-specific vulnerability assessments, and global threat intelligence, the SIEM's forensics capabilities are further augmented.

In time, Stratecast anticipates that intelligence sharing will become bi-directional, so that that SIEM-collected and processed intelligence is incorporated into the forensics processes of ThreatMatrix. This approach is important for automated incident responses to become more prevalent, either directly through ThreatMatrix or through its integration partners.

Ambition

Strongly fitting into this attribute is the upcoming Attivo ThreatPath feature. The noteworthy aspect of ThreatPath is threat prevention. With ThreatPath, threat prevention is accomplished by: (1) continuously and transparently gathering information about the customers' production network, systems, and devices via dissolvable or persistent agents; (2) combining that information with knowledge of attacker behaviors accumulated by Attivo; (3) defining the pathways attackers would likely follow; and then (4) producing high-fidelity incident prevention recommendations back to the customer, which correspond to those likely pathways to vulnerable assets. Figure 2, shows a screenshot of ThreatPath mapped assets. **The ambitious aspect of ThreatPath is in advancing the security value of Attivo from its initial core value of deception-improved *incident response* to the proactive *incident prevention*.**

Figure 2: Attivo ThreatPath



Menu > Critical Paths > 10.16.1.209 - 192.168.1.213

banappwebserv01
10.16.1.209
AD Path: MyCompay > ITApps > APAC > Bangalore
Last Checked: Mon Jul 11 2016 14:35

Exposed Credentials

RDP	CORPDC/svcacct-DC	Very High
RDP	CORPDC/svcacct-DC	Very High
RDP	CORPDC/svcacct-DC	Very High

Vulnerabilities

Presence of local administrative privileges for a domain user account	Very High
Lack of disable policy for account delegation right for privileged accounts	High
Presence of open file shares	Medium

Source: Attivo Networks

Stratecast
The Last Word

Cybersecurity has been referred to as a “cat and mouse” game where each party seeks to outmaneuver the other. As one makes a proactive move, the other party makes a countermove, and vice versa. In reality, however, this metaphor is only partially accurate as only one of the parties, the attacker, is initiating new moves; and the other party, an organization with digital assets, is in a perpetual state of reaction: that is, responding with countermoves. As this unidirectional, move and react game continues, the organization’s countermoves or countermeasures fortunately have an impact on the attacker’s effectiveness; until the attacker devises new moves that either partially to fully negate those countermeasures; or devises new moves that exploit other vulnerabilities in the organization’s networks, systems, applications, devices, and user community. The organization, however, is again faced with the reactionary need to overlay new countermeasures. Such has been the condition of cybersecurity.

Deception, in its present incarnation, is a promising means to recast this serious game from unidirectional to bidirectional. By exploiting the attacker’s vulnerabilities—thirst for information and initial blind approach to information gathering—the organization improves its ability to identify, with certainty, attackers; and, unknowingly to the attackers, move them away from real assets. Not knowing they have been deceived or how they have been deceived, the attackers are, in a manner of speaking, penned in.

Michael Suby

VP of Research

Stratecast | Frost & Sullivan

msuby@stratecast.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.