CALCULATING ROI FOR ATTIVO DECEPTION AND CONCEALMENT TECHNOLOGY
Cybersecurity professionals understand the value of deception technology. Unfortunately, while they may have input when determining the merits of security solutions to purchase, they do not often have the authority to influence budgets, which means that they must find a way to financially justify a new security technology to the CFO and others. How can they clearly explain the value? How will it save money? How reliable is this technology? Security teams must almost certainly answer these questions for those who can justify funding the purchase. Fortunately, quantifying the value and cost savings associated with deception technology is not as difficult as it may seem, especially when combined with concealment technologies. The following discussion will demonstrate the return on investment and cost savings related to deception solutions. Concealment technology serves as a prevention control as attackers will no longer have the ability to see or access the critical data they need to conduct an attack. Although this paper does not directly cover the savings shown in the research, the technology will serve to amplify the savings from avoiding the attack altogether.

**REDUCING DWELL TIME**

The amount of time that an attacker remains hidden before discovery (what is known as “dwell time”) directly correlates to the cost of a breach and the operational costs associated with remediation. The longer the dwell time, the greater the costs. According to current security industry research, dwell time ranges from 56 days to over 200 days, depending on the study. A recent survey conducted by Enterprise Management Associates found that the respondents most familiar with deception technology reduced their average dwell times to fewer than six days, reflecting a 90-97% reduction and a measurable drop in the costs associated with the breach and subsequent remediation.

---

**EMA Research “A Definitive Market Guide to Deception Technology” published August 2019**

What was the longest approximate time in days it took to detect a threat inside your network (a.k.a. average dwell time)?

- Deception Users with High Familiarity: 5.52 days
- Deception Users with Good Familiarity: 11.09 days
- Deception Users with Limited Familiarity: 6.94 days
- Non-Deception Users: 60.93 days
- All Respondents: 31.93 days

Mean Time to Detect in Days
BREACH SAVINGS

According to IBM's 2020 Cost of a Data Breach Report, the average cost of a data breach is now $3.86 million worldwide, with that number rising to $8.64 million for those in the US. Reducing attacker dwell times results in a reduced impact and associated cost, as breaches with lengthier dwell times tend to be more severe. Reducing dwell times by using deception technology solutions results in a cost-of-breach savings of as much as 51%, or an average of $75 per compromised record.

SOC OPERATIONS

Alert fidelity statistics indicate that as many as one in three alerts generated by traditional detection solutions are false positives. These false alarms are a waste of time and resources as SOC analysts must treat all events as positives until they determine their veracity. Recent research conducted by Deceptive Defense, Inc. highlights the value in SOC operations savings. Deception technology can reduce SOC inefficiencies by as much as 32% (or $22,747 per SOC analyst per year) based on alert fidelity substantiated with information like TTPs and IOCs, along with forensics collected during engagements that can significantly reduce attack investigation and response time.

<table>
<thead>
<tr>
<th>SOC ACTIVITY</th>
<th>TIME %</th>
<th>ATTIVO $ BASED ON $70K SALARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizing/planning detection and evaluation of suspicious events</td>
<td>12%</td>
<td>$8,285.54</td>
</tr>
<tr>
<td>Gathering actionable intel about cyber threats and vulnerabilities</td>
<td>11%</td>
<td>$7,901.16</td>
</tr>
<tr>
<td>Evaluating actionable intel</td>
<td>10%</td>
<td>$7,217.82</td>
</tr>
<tr>
<td>Investigating actionable intel and building incident timelines</td>
<td>15%</td>
<td>$10,677.24</td>
</tr>
<tr>
<td>Cleaning, fixing, or patching networks, applications, and devices</td>
<td>18%</td>
<td>$12,257.47</td>
</tr>
<tr>
<td>Documenting security incidents</td>
<td>8%</td>
<td>$5,552.17</td>
</tr>
</tbody>
</table>
Deception solutions capable of automating attack analysis, correlating events, and providing built-in native integrations can also reduce incident response time through automation. These integrations automate endpoint isolation, network blocking, intelligence sharing, and threat hunting. Attivo Networks provides over 40 native integrations with leading endpoint, firewall, SIEM, and SOAR platforms that it can leverage for automation. Attivo customers that utilize the automated attack analysis and response automation capabilities have commonly cited a 12- to 15-fold reduction in time that it takes them to investigate and remediate an incident.

**RANSOMWARE DETECTION**

Another factor to consider is the loss associated with ransomware attacks. Research shows that recovering an endpoint from a ransomware attack costs anywhere from $436 to $1,726 per endpoint, depending on the number of affected systems. Deception and technology can reduce the effects of a ransomware attack by alerting on such activity early, redirecting the attack to decoy file shares and data, and slowing the attack by up to a factor of 25. Reducing the number of affected systems corresponds to a drop in recovery costs compared to the investment in deception technology.

Attivo has created a Ransomware ROI Calculator to assist organizations when comparing investment in Attivo solutions versus the projected cost of recovering from a ransomware breach. For example, an organization with 1,000 endpoints and 200 servers that expects a ransomware attack once a year at a 15% infection rate would see a 68% annual ROI investing in Attivo solutions versus paying the ransom for 240 impacted systems, and an 86% ROI when compared to recovering them. To see the calculator in action, please visit https://attivonetworks.com/request-demo/ and specify in the notes section that you would like to see a demonstration for the Ransomware ROI Calculator.

Deception and Concealment technology can reduce the effects of a ransomware attack by alerting on such activity early, redirecting the attack to decoy file shares and data, and slowing the attack by up to a factor of 25.

**INSIDER THREAT DETECTION**

Cyber deception can be remarkably valuable for insider threat detection. Its ability to non-intrusively detect policy violations as well as nefarious activities sets it apart from other solutions. The Enterprise Management Associates (EMA) study recognized deception as the most efficient security control for detecting insider threats. Investigation teams point out that using cyber deception for incident response generates engagement-based alerts that substantiate unauthorized activity detection. This substantiation can eliminate hours, days, or even weeks that they would typically spend confirming an attack pattern or that the detected activities were indeed an incident.

**VALIDATING ROI WITH MITRE ATT&CK AND SHIELD**

The MITRE Corporation Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Matrix provides a model for cyber adversary behavior, reflecting various phases of an adversary’s lifecycle and the platforms they are known to target. The framework aims to help determine which technologies work or fail, identify gaps to improve security
posture and processes, prioritize work on detecting and deterring techniques, and evaluate new security technology. ATT&CK is useful for understanding security risk against known adversary behavior, planning security improvements, and verifying that defenses work as expected. The goal of ATT&CK is to break down and classify attacks clearly and consistently, making it easier to compare them to find how the attacker exploited networks and endpoints in a successful compromise. Research with MITRE’s Do-It-Yourself evaluation tools has shown that deploying Attivo deception and concealment technologies in conjunction with an Endpoint Detection and Response solution results in a 42% increase in detection effectiveness.

MITRE has also created a knowledge base named Shield that captures capabilities surrounding Active Defense and adversary engagements. Shield complements the MITRE ATT&CK knowledgebase mentioned above. From a defender’s perspective, the ATT&CK matrix provides a data model for protecting an enterprise against cybersecurity threats. Meanwhile, the Shield matrix provides the capabilities a defender must build for an Active Defense and adversary engagement in a post-breach situation. Deception and concealment technologies figure prominently in Shield, such that many of the Active Defense techniques reference it directly. Attivo’s deception and concealment technologies can cover 27 of the 33 techniques within Shield, as well as over 120 of the 190 documented use cases. To learn more about how the ThreatDefend® platform capabilities map to the Active Defense techniques and use cases in the MITRE Shield knowledge base, see here.

AUGMENTING DECEPTION WITH CONCEALMENT

Most of the research associated with demonstrating the value and savings of deception technology focuses on quickly detecting attackers using lures or decoy traps that reveal their presence when they attempt to engage. However, one can generate additional savings by augmenting deception technology with concealment technologies.

Concealment technologies work differently than typical deception. Instead of interwoven decoys and lures spread throughout the network to detect and snare the attacker, concealment solutions center on attack prevention. They operate by hiding and denying access to real objects on the network. For example, security teams could apply concealment technology around Active Directory. When attackers attempt to query Active Directory, the technology feeds them fake information. It also immediately alerts the defenders, and, should the attackers use any of this deceptive data, it diverts them into a decoy environment. Because the attackers won’t be aware that they are engaging with decoys, they continue to carry out their attacks, revealing their methods and attack strategies to defenders.
Concealment technologies can also hide the local data that attackers are after. Using concealment technologies, defenders can hide files, folders, network and cloud shares, and removable drives so the attackers will not find or alter the data they are seeking. The attackers cannot steal, encrypt, or otherwise tamper with data if they cannot find it. This capability is particularly useful against ransomware infections. Since the ransomware can’t access the local data, they can’t encrypt it, preventing further damage in conjunction with the deceptive file shares and data the malware encrypts.

DECEPTION AND CONCEALMENT COMBINE TO PROVIDE INCREDIBLE VALUE

Today’s information security landscape demands a layered defense, but justifying the value of any single security control is always a challenge. As security professionals, CFOs, and other vital decision-makers recognize, there is no such thing as a silver bullet or a one-size-fits-all solution. As shown by evaluating the Attivo solutions with the MITRE ATT&CK® and Shield frameworks, there is a demonstrable boost in performance and detection coverage. Attivo’s deception and concealment technologies can provide real, tangible, bottom-line benefits to organizations that choose to use them.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.