Deceptive
Defense, Inc.

CYBER DECEPTION SIGNIFICANTLY REDUCES DATA BREACH COSTS & IMPROVES SOC EFFICIENCY

AUGUST 2020

Sponsored by

Attivo
NETWORKS

SUMMARY

Cyber deception provides organizations with a high-fidelity, low-noise attack detection solution that not only reduces the cost of data breaches, it increases the efficiencies of typical Security Operations Center (SOC) operations, thereby providing direct and measurable financial benefits for organizations of all sizes and types. Compared to organizations that don't leverage deception technology, those using cyber deception can see the cost of a data breach reduced by over 51%, resulting in an average reduction in data breach costs of $1.98 million per incident or $75.12 per compromised record. In addition, increased SOC efficiencies can save organizations as much as 32% or $22,746 per SOC analyst per year.

DECEPTION TECHNOLOGY CAN REDUCE THE COST OF A BREACH BY OVER 51% AND CAN REDUCE PER ANALYST SOC COSTS BY 32%

THE DETECTION PROBLEM

Traditional cyber-attack detection methods look for signatures or indications of "evil" in our computing environments. Unfortunately, many attackers are able to make "evil" appear "not evil" to avoid detection. This is confirmed by both the 2020 Ponemon Institute Cost of a Data Breach Study and the 2020 FireEye M-Trends report. According to FireEye, the median amount of time an attacker is present on a victim network before detection is 56 days, while the Ponemon study put that number at 207 days. *Note: the large difference between the Ponemon and FireEye is likely due to different sample sizes. The M-Trends report is compiled based on incidents handled by FireEye while the Ponemon report involves a broader sample of organizations. Regardless of the reference you choose, dwell time remains a challenge and the longer the attacker can remain undetected the more costly the incident becomes. Any dwell time measured in days is far too long for an attacker to be inside your network. For this reason, early and accurate detection with a focus of reducing dwell time down to hours should be a priority for every organization.*

MEDIAN DWELL TIME – 56 DAYS

2020 FireEye M-Trends

MEAN TIME TO IDENTIFY – 207 DAYS

2020 Ponemon Institute Cost of a Data Breach Study

THE DETECTION SOLUTION – CYBER DECEPTION

Cyber deception involves placing resources on a network that will either obfuscate production devices amongst decoys or conceal and deny access to data. Its sole mission is to accurately detect and derail in-network threat activity early in the attack cycle. As a result, there should be no disruption to operations or legitimate interaction with these resources. Any interaction is considered abnormal and thus should be investigated as a priority alert. Because these interactions can generate a significant quantity of company-centric incident intelligence, the ability to both detect quickly and respond effectively is significantly improved, which can have a beneficial impact on both the cost of the breach and in terms of SOC efficiencies.

CYBER DECEPTION BENEFITS FROM DATA ASSET INVENTORY, DATA CLASSIFICATION AND EFFECTIVE

Properly deployed deception can reduce a company's average dwell time down to as little as 5.5 days, though many will cite verified detections within minutes. Depending on whether you reference Ponemon or FireEye, this results in an average reduction in dwell time of between 90% and 97%. The alerts generated by cyber deception are also found to be not only earlier but also more reliable than traditional detection solutions. As much as one out of three alerts generated by traditional detection solutions are false alarms or "false positives". And according to The 2020 edition of the *Mandiant Security Effectiveness Report*, alerts are only generated from 9% of attacks, further delaying the detection and remediation of threat activity. While false positives can occur with deceptive detection, this is rare and would typically only occur when there is a misconfigured network device or improperly configured white-listings. The alerts generated by deception technology are also categorized as high-fidelity as they include detailed intelligence about the attack and the attacker. Thus, the ability to respond more effectively is significantly increased while the time it takes to identify false positives is significantly reduced. Finally, when compared to the combination of system/device logs, IDS, IPS, DLP, and/or SIEM technologies, cyber deception is much simpler to design, deploy, and operate.

CYBER DECEPTION CAN REDUCE DWELL TIME BETWEEN 90% AND 97% - TO AS LOW AS 5.5 DAYS

Optimal efficacy of cyber deception can be achieved via some beneficial security practices, data classification and incident response. When deploying cyber deception, it is important that organizations understand what resources are on their network and the relative value of those resources to the organization. The combination of a detailed data-asset inventory and an effective data classification program are thus often combined with the deployment of deception technology. It's important to note that the machine-learning that is used to match decoys to production assets can aid in the inventory and visibility to devices on the network and their configurations. Similarly, because cyber deception is largely focused on attack detection, deception solutions should be combined with comprehensive and tested incident response capabilities. Fortunately, both data classification and effective incident response result in measurable benefits that further increase the overall value of a cyber deception initiative.

According to the 2020 Ponemon Institute Cost of a Data Breach Study, the average cost of a breach is $3.86 million or $146 per compromised record. That same study identified factors that can increase or decrease data breach cost, many of which are benefits achieved by the effective use of deception technology as shown in the following table:

Effect of Deception Technology on Data Breach Cost		Breach Cost (Millions)	Per Record Cost (US Dollars)
Average Data Breach Cost		$3.86	$146.00
Method	**Reduction in Cost Percentage**	**Reduction in Cost US Dollars (Millions)**	**Reduction in Cost per Compromised Record US Dollars**
Faster Detection and Response	29	$1.12	$42.34
Effective Incident Response	14.8	$0.57	$21.68
Reduced Complexity	7.6	$0.29	$11.10
TOTAL	**51.4**	**$1.98**	**$75.12**

SOC INEFFICIENCIES

According to a March 2020 article in *Secure Computing Magazine*, on average, 26% of alerts are false alarms or "false positives". According to the Ponemon Exabeam SIEM Productivity Study, 33% of alerts are false positive. These numbers are reinforced by an article on helpnetsecurity.com (https://www.helpnetsecurity.com/2019/08/29/soc-alert-overload/), that says 45% of responding organizations stated that 50% or more of alerts were false positives.

The SIEM Productivity Study also found that the average amount of time spent per SOC analyst per incident was around 10 minutes. According to a study conducted by EMA entitled "A Day in the Life of a Cyber Security Pro" found that analysts were spendingbetween 24 and 30 minutes investigating each alert. Additionally, the SIEM Productivity study found that SOC analysts waste approximately 26% of their day dealing with false alarms. Using an annual salary of $70,000 for a SOC analyst, this represents a loss of over $18,000 in productivity per analyst per year. By reducing the number of false positive alerts, this productivity loss can be significantly reduced or virtually eliminated.

25% TO 33% OF ALERTS ARE FALSE POSITIVE, WASTING OVER $18,000 PER SOC ANALYST ANNUALLY

These savings are provided in context to how analysts spend their time addressing the following activities:

SOC Activity	Time %	$ Based on $70K Salary
Organizing/planning detection and evaluation of suspicious events	12%	$8,285.54
Gathering actional intel about cyber threats and vulnerabilities	11%	$7,901.16
Evaluating actionable intel	10%	$7,217.82
Investigating actionable intel and building incident timelines	15%	$10,677.24
Cleaning, fixing and/or patching networks, applications, and devices	18%	$12,257.47
Documenting security incidents	8%	$5,552.17

Source: SEIM Productivity Study

Just as cyber deception can reduce time wasted on false positive alerts, the high fidelity and low noise of deceptive detection solutions, combined with increased attack intelligence, can also streamline many of the other SOC processes. Users of deception technology have cited a 12X time savings when addressing a deception-based alert as opposed to other alerts. While documentation of security incidents is unlikely to be significantly affected by the use of deception technology, all other SOC activities will see increased productivity. Assuming such an increase amounts to a modest 10% increase in efficiency, this can reduce SOC costs by an additional $4,600 per analyst per year for a total per analyst savings of almost $23,000 per year or a decrease in SOC analyst costs of 32%.

The combination of detecting attacks early, reducing the cost of a data breach by an over 60%, and improving SOC efficiencies by 32% can result in significant savings for organizations both large and small. When paired with the ability to boost EDR detection rates by over 42%, according to testing with the MITRE ATT&CK® framework DIY tool, this can be a powerful security control to add to every defender's arsenal.

This report is sponsored by:

About Attivo Networks

Attivo Networks®, the leader in cyber deception and attack lateral movement detection, delivers a superior defense for revealing and preventing insider and external unauthorized threat activity. The Attivo ThreatDefend®Deception Platform provides a scalable, customer-proven platform for derailing attackers within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio includes its flagship BOTsink® deception solution and the Endpoint Detection Net and ADSecure products, which deliver ground-breaking innovations for preventing and misdirecting attack escalations. Incident response is streamlined with forensics, automated attack analysis, and third-party native integrations.
The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.

WITH DECEPTION TECHNOLOGY

Reduce data breach costs by 51.4% - average savings of $1.98 million per incident or $75.12 per compromised record

Reduce SOC inefficiencies for a reduction in SOC analyst costs by 32% - average savings of $22,746 per analyst per year

Deceptive
Defense, Inc.