Beginner’s Guide To Cyber Deception
Executive Summary

Cyber threats are increasing in both frequency and severity, defenders are challenged to maintain defense of rapidly evolving IT infrastructures, and even best practice defense-in-depth security strategies are no guarantee against being the next victim of cyber attack. Cyber deception solutions have matured in recent years to allow security teams to take a more proactive stance against attackers by leveraging a variety of deception approaches, including honeytokens, honeypots, and breadcrumbs. These technologies exist to misguide and identify attackers attempting to navigate and breach a target environment.

Organizations that include cyber deception as a component of their defense-in-depth strategies can expect to achieve earlier discovery of compromise, increased detection accuracy, and more relevant and actionable threat intelligence. These benefits do not come without challenges, however. The following are key issues organizations are likely to expect when implementing a cyber deception solution:

1. Complexity of deploying, configuring, and managing the cyber deception solution.
2. Ability to achieve the required scale - both from an infrastructure and skilled personnel perspective.
3. Increased overall risk resulting from potentially insecure cyber deception solutions.

To address the challenges facing traditional cyber deception products, vArmour has created the industry’s first simple, scalable, and secure cyber deception solution: vArmour DSS Deception. By leveraging vArmour’s patented distributed architecture and micro-segmentation technologies, security teams are able to achieve a proactive security posture while simultaneously streamlining workflows and reducing overall risk.
Background

Deception as an element of cyber defense is not a new idea. In fact, cyber deception products have been available for nearly 20 years and were instrumental in combating the widespread proliferation of computer worms in the early 2000s. So why have cyber deception technologies not been more widely adopted in the subsequent years? Why is there now a resurgence of interest in deception? What has changed so that organizations big and small are now seeking out cyber deception technologies to better secure their environments? Three major components driving these changes are: increasing risk, evolving IT infrastructures, and an uneven playing field for defenders.

Increasing Risk

The constant barrage of attacks facing modern organizations is no longer a revelation. However the frequency and severity of these attacks has certainly increased dramatically in recent years. As attackers have become much more sophisticated in their target selection, detection evasion, and monetization of breached data, the task of defending an organization’s IT infrastructure has become far more difficult and critical to the organization overall.

Attackers and the malware they utilize have become increasingly vicious as well. For example, targeting the healthcare sector and holding organizations’ data hostage with ransomware has become a common tactic. In attacks not motivated by monetary gains (e.g. retaliation, ideology, media exposure, etc.), attackers can be even more damaging. In the attack against the Sands Casino network in early 2014, though not publicized as widely as other breaches, attackers simply destroyed all the data on every computer they could locate on the network. Roughly three quarters of the organization’s servers in Las Vegas were erased with an estimated cost of rebuilding the systems at $40 million, not to mention the lost revenue and brand damage.¹

Evolving IT Infrastructures

Adding to these challenges is the rapid evolution of today’s IT infrastructures. Virtualization and public cloud infrastructures, which were cutting edge only a few years ago, are already giving way to containers and multi-clouds. Organizations are quickly moving to adopt these new infrastructures in order to take full advantage of the flexibility and agility they provide. Although a great enabler for the organization, these advancements present some significant challenges for security teams.

Emerging Threat Surfaces

First, the rapid evolution and adoption of new IT infrastructures means that security teams are racing to keep up with the security implications and differing attack surfaces of each new technology. The prevailing philosophies of mobile computing, BYOD, and IOT continue to dissolve traditional security architectures and move digital operations outside the perimeters of corporate networks and data centers. This is made even more complex with the all too frequent utilization of “shadow IT,” or teams utilizing public cloud or SaaS offerings unbeknownst to the organization’s IT and security teams.

Increased Time Pressures

Second, new flexible IT infrastructures allow organizations to operate with more agility so projects that previously would have taken months of planning and provisioning can now simply be spun up in a matter of days. This means that the security teams do not have the same window of time to review the plans and design an appropriate corresponding security strategy. They instead are forced to operate without full context in ever-shifting and dynamic environments. The most mature security programs have influenced their organizations to implement orchestrated security provisioning throughout the software development lifecycle, though this is sadly out of reach for most security teams.

Growing Blind Spots

Third, the agility afforded by today’s IT infrastructures comes via layers of abstraction on top of traditional hardware. This provides tremendous flexibility, but it is not without its drawbacks.
Historically, security teams operated with a fair amount of visibility into their networks and data centers by collecting logs from servers, network devices, and security products. The blind spots of intra-subnet and intra-VLAN traffic, although significant problems, were accepted primarily because there were no reasonable solutions available. Today’s new IT infrastructures amplify this problem by creating additional layers of abstraction with little to no visibility within the new layers. Or to put it another way, yesterday you could not easily inspect the communications between two servers on the same subnet. Today, you cannot easily inspect the communications between the hundred or more virtual machines or containers hosted on those two servers.

### An Uneven Playing Field

It goes without saying that today’s attackers continue to be able to achieve their goals in these new environments. By almost every measure, attackers continue to operate with near total freedom while security teams struggle to keep up:

- The median amount of time attackers are able to operate undetected in a target environment is 146 days.\(^2\)
- The number of records compromised in breaches in 2015 was 153 million - a 128% increase from 2014.\(^3\)
- A smaller percentage of breaches is discovered by defenders year-over-year - down to roughly 17%.\(^4\)
- 76% of organizations were affected by successful cyber attacks in 2015.\(^5\)
- The average cost of a breach is $3.79 million - an increase of 23% since 2013.\(^6\)

In short, cyber threats are increasing in both frequency and severity, defenders are challenged to maintain defense of rapidly evolving IT infrastructures, and even best practice defense-in-depth security strategies are no guarantee against being the next victim of a cyber attack. So what else can security teams do to help level the playing field?

---

Introduction to Cyber Deception

In the field of cyber security, deception means making someone (an adversary - either external or internal) believe something that is not true in order to better defend the target environment (network, data center, server, etc.). This is markedly different from traditional security defenses, which are almost universally designed to monitor legitimate data (files, network communications, memory) and watch for suspect activity. This is often referred to as “finding the needle in the haystack” to illustrate the challenge in accurately locating and identifying a small amount of suspect data contained within such vast amounts of legitimate data.

Cyber deception, by contrast, is not intended to spot suspect data within a sea of legitimate data. It is instead intended to create situations where no legitimate data, traffic, or activity should ever occur, but that appears enticing to an adversary. In this way, whenever there is any activity, traffic, or access to the deception, it can immediately be classified as suspicious.
Rather than trying to find a better way to find the needle in the haystack, deception aims to bring the needle outside the haystack so it's easier to find.

This does not mean that cyber deception techniques are a replacement for traditional approaches to security. For example, removing the perimeter firewalls, intrusion detection/prevention systems (IDS/IPS), web application firewalls (WAF), and security information and event managers (SIEM) from an environment once a cyber deception solution had been installed certainly wouldn’t improve overall security. However, as attackers and their tactics are becoming ever more sophisticated, even a small blind spot or missed attack can result in millions of dollars in lost revenue, brand reputation, remediation, and potential fines. Therefore, relying solely on traditional security tools and approaches carries significant, and increasing, risk. In fact, in many of the breaches that are publicized in the media, it is not the case that those organizations did not have any security solutions in place, but rather that the attacks slipped by those detection systems or it was identified but lost in a sea of alerts that would have taken too long to review.
Cyber Deception Technologies

The category of cyber deception describes the intent of the security practitioner rather than a specific method or tool to be used. As such, there is a vast collection of tools and techniques that can be classified as cyber deception technologies. From a database of fake credit card numbers to networks that synthesize slow or poor connectivity, anything that intentionally manipulates the attacker’s experience of the environment and their progress toward their objective qualifies as a cyber deception technology.

Given the large number of tools and techniques for cyber deception, there is some disagreement across the industry on standard terms and categories with some tools and products crossing categories or not fitting into any at all. Though not an exhaustive list of cyber deception approaches, the following is a collection of a few of the most common deception terms and what they mean.
Honeytokens

Honeytokens are uniquely identifiable data entries (credentials, data records, or specially crafted byte strings) that are injected into legitimate data (documents, databases, source code, email lists, etc.) and are then monitored to identify access to or transmission of the data. These fake data entries are designed specifically to identify unauthorized use or transmission of the data they reside in.

For example, a credential might be created within an Active Directory system that is never intended to be used by any actual person or system. By monitoring for authentication attempts using this credential, security teams are able to know that the Active Directory system has been compromised. It can be helpful to think of honeytokens as the canaries in the coal mines throughout an environment. By attempting to use the data that has a canary monitor, the attacker is unknowingly revealing both their presence and the data they have access to.

Honeypots

A honeypot is a real or synthesized computer system, application, or service that appears to be legitimate, but is in fact only utilized for luring, identifying, and analyzing adversaries. A honeypot may be a stand-alone system, an individual service on a workload, or a local software agent to name a few possibilities. By monitoring access to or use of these decoy systems, security teams are able to identify adversaries inside the target environment because no legitimate user, application, or process would ever need to access these fake systems.

Honeypots are also utilized externally where they can receive communications from the open internet. In this scenario, honeypots are most commonly used in a research capacity for identifying new attack vectors, malware samples, and general intelligence gathering on attacker techniques. When security vendors claim to have “sensors spread across the internet,” this is generally what they are referring to.

As an example, an organization concerned with protecting their intellectual property that is housed on a particular workload might deploy additional decoy workloads that resemble the original at various points in the data center. This effectively hides the critical workload in a collection of copies. Legitimate users will know exactly which workload is the real one, but adversaries will be led to believe they are all legitimate. As soon as an adversary attempts to access one of the decoys, security teams are alerted to the adversary’s presence.
Honeypots

A honeypot is a real or synthesized computer system, application, or service that appears to be legitimate, but is in fact only utilized for luring, identifying, and analyzing adversaries. A honeypot may be a stand-alone system, an individual service on a workload, or a local software agent to name a few possibilities. By monitoring access to or use of these decoy systems, security teams are able to identify adversaries inside the target environment because no legitimate user, application, or process would ever need to access these fake systems.

Honeypots are also utilized externally where they can receive communications from the open internet. In this scenario, honeypots are most commonly used in a research capacity for identifying new attack vectors, malware samples, and general intelligence gathering on attacker techniques. When security vendors claim to have “sensors spread across the internet,” this is generally what they are referring to.

Two or more honeypots that intercommunicate are often referred to as a honeynet. As an organization deploys a number of honeypots to provide adequate coverage across an environment, configuration, monitoring, and management become a pain point. Honeynets attempt to alleviate this by networking the various honeypots together into a single unit.

Breadcrumbs

Breadcrumbs are references to fake systems, credentials, services, etc. deployed across legitimate systems in order to both make the deceptions appear more legitimate and to attempt to steer attackers toward those deceptions. Breadcrumbs often take the form of log entries, web bookmarks, or other common references to systems or data.

Breadcrumbs are designed to address one of the historical shortcomings of cyber deception technologies, particularly honeypots. A cyber deception solution can be extremely accurate and effective, but only if the attacker sees and interacts with that deception. In large networks and data centers, the chance of an attacker stumbling upon a honeypot is relatively small, so breadcrumbs are a way to try and point attackers in the right (wrong) direction.

Expanding on the previous honeypot example, the organization may wish to make the decoy workloads appear even more legitimate and try to further drive attackers away from the legitimate critical workload. To do this, they could deploy breadcrumbs - for example fake log entries on workstations or other servers - that reference the decoys. By creating artifacts throughout the environment that appear to be the result of legitimate use of the decoys, the organization is able to further steer adversaries away from the critical asset.
Putting It All Together

Given the range of cyber deception technologies and the varied ways they are implemented and benefits they provide, it can be challenging to know where to start. To summarize the previous section:

- Honeytokens reside in legitimate systems already in existence and function as an alarm that suspicious access or misuse has or is currently happening.
- Honeypots are the workhorse of most cyber deception solutions. They are both the traps set for attackers as well as the collection mechanism for threat intelligence.
- Breadcrumbs are a mechanism for driving traffic to honeypots as the significant coverage from honeypots can be extremely challenging (or costly) to achieve.

From this information, we can understand why a common strategy for introducing deception into a security program is to start with honeytokens and honeypots since breadcrumbs serve no purpose if there is no honeypot to drive traffic to. Honeytokens can be implemented fairly easily without a full blown cyber deception solution as the fake data or credentials reside on legitimate systems. It is trivial to create fake email addresses or user credentials and then monitor for their use, which leaves the bulk of the heavy lifting to honeypot solutions. The remainder of this paper will focus on the benefits and challenges security teams are likely to encounter when implementing a honeypot-based cyber deception solution.
The changing dynamics discussed at the beginning of this paper provide a somewhat stark backdrop to the tasks facing security teams today. With increasing complexity, changing infrastructures, and advancing attackers, what demonstrable benefits can cyber deception technologies deliver? Where, specifically, can cyber deception technologies move the needle for security teams? Cyber deception allows security teams to shift their thinking and strategizing from being purely reactive to proactive, but what are the resulting quantifiable changes? There are many benefits to including deception as a component in a defense-in-depth security strategy, but earlier compromise discovery, increased detection accuracy, and more relevant and actionable intelligence are three of the most common goals for security teams.
Earlier Compromise Discovery

Fewer than one in five publicly disclosed breaches are discovered by the breached organization itself, with the remainder being discovered by law enforcement or by the exfiltrated data appearing on the black market. For attacks that are discovered by the breached organization, a significant portion are identified during or immediately after the attacker is exfiltrating the data out. Obviously the prospect of uncovering a compromise earlier is highly desirable, so how do cyber deception technologies achieve this?

Nearly all security solutions are designed to identify attacks that are either in progress or have already happened. Intrusion detection/prevention systems (IDS/IPS), web application firewalls (WAFs), data loss prevention (DLP), security information and event managers (SIEMs), and nearly every other security product available generates alerts when an attack is currently taking place or when an adversary is exfiltrating the data they’ve already collected. Although this is extremely valuable and necessary from a defense-in-depth perspective, it would be far preferable to be notified before an attack against a legitimate system was taking place. Using a cyber deception solution, alerts can be triggered simply when an adversary attempts to access the deception, providing a far earlier warning for security teams than relying purely on non-deception security solutions. Moreover, by engaging with and identifying attackers using decoys, defenders are simultaneously slowing any potential breach timeline as the attacker is not accessing a legitimate system.
Increased Detection Accuracy

Attackers have become quite skilled in evading traditional detection solutions. Since an attacker’s activities are surrounded by vast amounts of legitimate traffic that detection solutions attempt to weed out (recall the needle in the haystack analogy), in order to better hide from security teams, an attacker must make their activities blend in and appear legitimate. This can be accomplished in a variety of ways including only using standard ports and protocols, breaking up large chunks of data into smaller files for transmission, scheduling activities to correspond with times of high network utilization, or many other techniques.

This results in large numbers of alerts generated that are triggered by legitimate traffic and activities (i.e. false positives). Cyber deception technologies change this dynamic not by creating more sophisticated detection logic, but by removing all the legitimate traffic the attackers hope to hide within. When an attacker accesses a honeypot, for example, they may be using a common protocol, transferring small files, during a time when the network is busy, but those techniques are irrelevant when they’re interacting with a system that no one should ever be interacting with. As a result, the alerts generated by the cyber deception solution have much lower false positive rates than their traditional security counterparts.
More Relevant and Actionable Intelligence

Threat intelligence is often touted as an integral component of any security strategy, however a common pitfall of most threat intelligence is that it is not relevant to the organization consuming the intel. The vast majority of threat intelligence is gathered either from the open internet, including external honeypots, hacker forums, and black markets, or from findings of other organizations who then share the data with others. These are not unreasonable places to gather intelligence, but with the increasing rise of attacks tailored to specific organizations, custom re-packing of malware to avoid detection, and various IP-hopping and domain generation algorithm schemes, the applicability of most externally generated threat intelligence is questionable.

What is really needed is intelligence on adversaries facing the specific environment or organization. Where are they located? What hosting infrastructure are they using? What types of tools are they leveraging? What are their objectives? This information is far more discernable from threat intelligence gathered internally than from broad-based intel or findings extrapolated from what a different attacker did in a different environment against a different organization. Though some of this internal intel can be gleaned from traditional security solutions (SIEM, IDS/IPS, WAF, etc.), it is far more secure to collect this intelligence through attacker actions directed at a deception rather than legitimate production systems.

Since the intelligence gathered by cyber deception solutions is far more specific and relevant to an individual organization than intel collected externally, the resulting analysis leads directly to more actionable findings. Cyber deception solutions allow security teams to accurately identify compromised workloads and credentials as well as collect the tools and malware being employed by the attacker. From there, it is a direct path to remediating the compromise by resetting credentials, determining the full scope of the compromise, and ideally quarantining the compromised workloads for secure forensic investigations.
Challenges of Existing Approaches

Since its inception nearly two decades ago, cyber deception technologies have evolved substantially, however it is a recent development that organizations are taking a closer look at implementing these technologies. Early on, cyber deception acquired a reputation of being only a “science project” or something that was an exciting concept but that was not ready for full deployment across production systems. At the very least, cyber deception technologies were not at the top of the priority lists for most security teams. This reputation is not all that surprising since cyber deception products have historically been extremely complex, time-consuming, and introduced new risks into the environments where they were deployed. Cyber deception vendors, particularly in recent years, have attempted to address these drawbacks by introducing more interconnected deception products and integrating with external orchestration systems and security information and event managers (SIEMs). Significant progress has been made, but the challenges have remained just enough to prevent most organizations from fully taking advantage of the benefits of cyber deception.

So what are the challenges facing modern cyber deception products? What causes them and how are those challenges likely to impact real world implementations of deception strategies? Arguably the three biggest challenges facing modern cyber deception products and the organizations wishing to implement them are complexity, scalability, and security.
Complexity

There are two primary methods for creating the appearance of endpoints across an environment. The first is to create fake endpoint systems (either physical or virtual), which are then deployed throughout an environment. This is the traditional honeypot approach. The second method is to install a software agent on every workload in the environment so that if a user or other process on the workload attempts to reach out to an address, application, or service configured as a deception, the software agent can interact as the fake destination or redirect the requests to another component of the deception system. Both approaches result in complex deployment, configuration, and management, though there are significant differences.

Traditional honeypot deployment scenarios incur complexity through the need for reasonable coverage across the network or data center.

As a single honeypot is unlikely to be stumbled upon by an attacker, the classic solution is to deploy more honeypots. This means that the more deception coverage you need, the more complex installations, configurations, and ongoing management are needed.

The alternate deployment method of placing software agents on every workload can appear to be a good option, but real world deployments tell a different story. Not limited solely to cyber deception, agent-based security solutions inherit a host of challenges of their own including support for legacy OSs, contention with other running agents, and consumption of compute resources on every workload. This complexity only compounds the challenges with deploying and managing a complex security program such as cyber deception.

Regardless of approach, coordinating communication and updates across dozens of honeypots or hundreds to thousands of agents is no small task. Although cyber deception vendors have made some progress in this area in recent years, excessive complexity is often cited as the cause for deception projects to stall or be canceled altogether. The end result is that only the largest enterprises with substantial infrastructure and security personnel resources tend to be willing to fully leverage cyber deception technologies.
To better quantify the complexity that accompanies most cyber deception deployments, the following exercises can be completed and used as inputs for choosing a cyber deception solution:

1. **Calculate the amount of cyber deception coverage required in the target environment.**
   
   Example questions:
   - Is the intended purpose of the cyber deception solution to identify attackers proactively or to opportunistically collect intelligence without the requirement for identifying larger numbers of adversaries?
   - What is the size of the environment needing cyber deception coverage?
   - Are all critical workloads and applications collocated in the same subnet, VLAN, or hypervisor to allow for easier networking, policy, and management coordination?

2. **Evaluate how well the different cyber deception deployment scenarios fit into existing IT and security policies and programs.**
   
   Example questions:
   - Are agent solutions shunned or embraced by the organization?
   - How heterogeneous is the environment to be protected? Are there non-standard or legacy operating systems in use?
   - If the organization’s IT strategy includes public or private cloud initiatives, does the solution support those environments natively?

3. **Determine potential dependencies.**
   
   Example questions:
   - Does a particular solution only integrate with particular operating systems or security solutions?
   - Are other infrastructure elements required in order to receive full value from the deception solution (e.g. SDN, containers, network visibility solutions)?
Scalability

As mentioned previously, achieving adequate coverage for a cyber deception solution within a network or data center is not a straightforward proposition. Simply adding more honeypots or deploying agents on every workload increases complexity, but an additional challenge is the resources required to operate these systems at scale - both infrastructure and personnel. Whether deploying honeypots or agents on every workload, the IT resources required to protect the environment scale linearly with the coverage achieved.

For honeypots, double the coverage (and double the chance an attacker will stumble upon the honeypot) means creating twice the number of honeypots with twice the compute, memory, storage, and network resources required. For agents, it is more a scenario of “death by a thousand cuts.” To achieve broad coverage with agents, every workload in the environment needs to be running the software agent. This impacts resources - compute, memory, storage, and networking - on every single workload. The more workloads in the environment, the larger the cumulative resources required to ensure adequate coverage.

The second aspect of scaling a cyber deception solution is the technically sophisticated security personnel typically required to operate and monitor what is a complex, strategic, and potentially risky system. With a projected shortfall of skilled cybersecurity personnel of 1.5 million by 2019, the pressure on organizations to both hire and utilize a skilled security team is only increasing.

With such intense staffing pressures, the prospect of spending a significant portion of those resources on potentially complex and time-consuming solutions becomes a much more difficult proposition.
In an ideal world, large scale cyber deception projects would be accompanied by equally large expansions in infrastructure and staffing resources. Unfortunately, this is rarely the case and, more often than not, additional security projects put further pressure on security teams to do more with less. The following can assist in evaluating required resources when choosing a cyber deception solution:

1. **Determine the amount of infrastructure resources the organization is willing to commit to a cyber deception solution.**
   
   Example questions:
   - Is it preferable to allocate a portion of the resources from every workload in the target environment or to assign a smaller number of full workloads as honeypots?
   - Does the addition of a cyber deception solution require additional hardware to be added to the data center? What additional capital and operational expenditures can be expected?

2. **Gauge the amount of personnel resources available for ongoing monitoring and investigation of cyber deception alerts.**
   
   Example questions:
   - Does the organization currently retain skilled security staff able to investigate and respond to cyber deception alerts?
   - Will additional infrastructure personnel resources be made available to support the project?
   - What portion of existing infrastructure personnel resources can be allocated for ongoing support of the cyber deception solution?

3. **Evaluate the available bandwidth and skill of the security personnel.**
   
   Example questions:
   - Is the skill level of the existing security team sufficient for monitoring and reacting to the given cyber deception solution?
   - Is monitoring and reacting to a cyber deception solution the best and highest priority activity for the available skilled personnel?
   - How feasible is it to assign less highly skilled personnel to working within the cyber deception solution?
Security

It may seem counterintuitive that implementing a security solution can increase the overall risks facing security teams, but this is a legitimate concern with regard to cyber deception solutions. For most security solutions, the proposition is to identify attacks occurring within the organization’s IT environment - to shine a light on attacks that would otherwise go undetected. Cyber deception solutions are different in that they are intended to be attacked directly, as the more interaction an attacker has with a cyber deception solution, the more intelligence can be gathered and the higher certainty the resulting security alerts can have.

In the case of agent-based deception solutions, security is particularly problematic as the agent processes intending to protect the workload reside on the same workload as the potential attacker. It is perhaps unsurprising that the first thing a savvy attacker will do after compromising a target workload is scan for and disable any local process for any security controls. This obviously renders any previous deception benefits null, but is arguably a preferable outcome when compared with the potential for the attacker to compromise the agent process and further spread, not to adjacent workloads, but to the security management network and systems themselves!

There are a handful of potential nightmare scenarios for security teams, but having attackers compromise the very systems they rely on for detecting, investigating, and remediating threats probably tops the list.

The situation for traditional honeypot deployments is slightly better in that attackers do not have direct access to the deception processes and only interact with the deception remotely. This removes the possibility that they can identify and disable the deception process and continue undetected. Those deception processes, whether appearing as full operating systems or a individual services, are still expected and intended to be attacked however. The resulting risk of compromise to the honeypot and subsequently the security management network remains a very real risk. It is possible to implement policy controls to secure a honeypot deployment, though it tends to multiply the complexity and scale challenges discussed above.
The security challenges involved in implementing a cyber deception program are arguably the single biggest objection encountered by security teams wanting to take a more proactive stance against adversaries. Understanding the organization’s risk tolerance as well as the risks associated with various deception implementations provides a good baseline for further cyber deception solution evaluation and selection. The following exercises can assist in determining these preliminary measurements:

1. **Weigh the risk potential of an undetected system breach compared with the added risk of a given cyber deception solution.**
   
   Example questions:
   - Would a breach be catastrophic for the organization?
   - Are there regulatory and/or legal implications associated with the organization’s data?
   - Does the cyber deception solution increase or decrease the overall risk to the organization?

2. **Evaluate the extent to which a cyber deception solution can be secured to alleviate additional risk.**
   
   Example questions:
   - What security controls are available natively within the cyber deception solution? In what scenarios can those controls be compromised or bypassed?
   - Can the solution be segmented to prevent a compromise from spreading beyond the local system?
   - Can visibility into network traffic - both incoming and outgoing - be achieved so any potential compromise can be identified and remediated quickly?

3. **Gauge the potential value of deceived attackers based on the types of adversaries expected to be faced.**
   
   Example questions:
   - Is the organization at a high risk of being attacked by sophisticated attackers?
   - What are the desired increases in detection accuracy and response times when compared to the existing security infrastructure?
   - To what extent will additional intelligence gathered by the cyber deception solution improve future efforts to track and identify adversaries?
vARMOUR DSS DECEPTION

As organizations continue to adopt new virtualization and cloud infrastructures in the face of escalating threat landscapes, the challenges facing security teams show no signs of abating anytime soon. vArmour DSS Deception is the industry’s first simple, scalable, and secure cyber deception solution; helping security teams achieve a proactive security posture while simultaneously alleviating the drawbacks of most cyber deception solutions.

Simple

The complex deployability, configuration, and ongoing management of most cyber deception solutions continue to prevent all but the largest enterprises from fully incorporating modern cyber deception technologies into their defense-in-depth security strategies. As data centers continue to transform leveraging more and more virtualization and software-defined technologies, security solutions are being pressured to keep pace in a new on-demand, fully orchestrated world. vArmour DSS Deception’s provides integrated and automated deployment, configuration, and management as well as powerful APIs for orchestration and workflow streamlining. Whereas most cyber deception solutions require complicated roll out plans and significant personnel resources, vArmour DSS Deception can be deployed and configured in as little as 15 minutes.

Scalable

To date, achieving sufficient scale with a cyber deception solution in all but the smallest environments has been tremendously challenging for security teams. By leveraging vArmour’s distributed security system architecture, however, massive scale can easily be achieved using an extremely small resource footprint. With a single Deception Point, vArmour DSS Deception is able to create the appearance of thousands of endpoint systems across unused IP address ranges in the data center, all without the use of endpoint agents. This massive deception coverage is made possible by
combining a single deception point with transparent traffic routing through the vArmour distributed system. The vast scale made possible by vArmour’s distributed architecture is unprecedented in the field of cyber deception solutions.

To enable security personnel to scale alongside their changing IT infrastructures and evolving threat landscapes, vArmour DSS Deception is integrated with vArmour Analytics allowing for deception, alerting, analysis, and, when combined with vArmour DSS Segmentation, remediation

Secure

vArmour’s approach to a secure cyber deception solution involves not only isolating the deception processes from attackers by not leveraging agents on individual workloads, but also protecting each Deception Point with extremely tight policy controls. Leveraging vArmour’s patented application-aware micro-segmentation technology, each Deception Point is only allowed to receive and send communications using a select few ports and applications. This dramatically reduces the attack surface available if an adversary was in fact able to compromise a Deception Point. What was previously a difficult and costly to achieve ideal - having tightly secured deception points by policy - is now a default with vArmour DSS Deception.

An additional benefit imparted by vArmour’s distributed security technology is full application-layer visibility into all traffic flows. This previously unavailable visibility into data center communications not only provides a treasure trove of information for security event analysis and incident response, but also full auditability and continuous monitoring capabilities for every Deception Point. No longer do security teams have to worry about whether their cyber deception solution has been compromised or whether they can trust the potentially compromised logging of deception events. With vArmour DSS Deception, Deception Point communications are independently logged up through Layer 7 and provide an objective view of the security of the Deception Point. By implementing vArmour DSS Deception, organizations can confidently move to a proactive security posture while simultaneously reducing risk in their data centers.
Get Started with vArmour DSS Deception

To learn more about how vArmour is addressing the challenges of traditional cyber deception solutions and creating the industry’s first simple, scalable, and secure cyber deception solution, visit www.varmour.com or register now to watch the webinar, Sending Attackers Down The Rabbit Hole: Introducing vArmour DSS Deception.

Watch the Webinar