STARVING YOUR ADVERSARIES:

PREVENTING ATTACKERS FROM LIVING OFF THE LAND BY SLASHING IDENTITY RISK

KNIGHTINK

AUTHOR INFORMATION
Alissa Valentina Knight
Partner
Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com

illusive

PUBLICATION INFORMATION
This white paper is in collaboration with Illusive, Inc.

Initial Date of Publication:
February 2022
Revision: 1.0

SUMMARY
This white paper was written for Chief Information Security Officers (CISOs) and other cybersecurity management as well as security engineers wanting to better understand the threat of subdomain takeover, what it is, how it works, and how an external attack surface management (EASM) tool plays a major role in thwarting these kinds of threats. Additionally, this paper goes deep into the threat of subdomain takeovers.

TABLE OF CONTENTS

TABLE OF CONTENTS

OVERVIEW

OVERVIEW

According to Centrify's Privileged Access Management in the Modern Threatscape survey published in 2019, 74% of IT decision makers surveyed whose organizations have been breached in the past, say it involved privileged access credential abuse. It's no wonder since there's been a five-fold increase in identities in the last decade alone (Identity Security Alliance, 2020)

> "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable." -Sun Tzu

The fact is indisputable. There is a direct linkage between increasing identity risk and breaches attributed to service and privileged account sprawl. As a result of the pandemic, employees have moved from their cubicles to their home offices while companies have moved assets and sensitive data into multi-cloud environments, leaving a trail of vulnerable identity breadcrumbs everywhere for adversaries to pick up and use.

These vulnerabilities include things such as service accounts capable of performing interactive logins over RDP, shared domain administrator accounts, cached privileged credentials on endpoints, policy gaps between on-prem Active Directory (AD) and Azure AD, and more.

While other security controls focus on detecting the symptoms of what happens when these connected and identity breadcrumbs are left scattered across a network, identity risk management (IRM) attempts to focus on preventing the cause by proactively reaching out to endpoints and disposing of cached credentials and Kerberos tickets, as well as stale and cached connections, so they can't be used by an adversary when a breach occurs.

IDENTITY RISK BY EXAMPLE

CNA Financial is among the largest insurers in the United States. In May of 2021, it was widely publicized that CNA had suffered a massive breach, falling victim to Phoenix Cryptolocker. It paid $40 Million in ransom, believed to be the largest ransom payout to date.

The Phoenix Cryptolocker ransomware, believed to be operated by Russia-backed Evil Corp, leverages a credential stuffing attack armed with usernames and passwords from previous breaches in order to attempt access to a network over RDP. The details of the compromise indicate that in CNA's case stolen credentials were used to gain a foothold on the network, from which the adversaries likely escalated privileges to Domain Admin.

As in all breaches, reconnaissance is the calm before the storm. The now infamous JBS Foods breach that followed shortly after the Colonial Pipeline breach began with RDP service mapping of the JBS network in Australia. While it couldn't be confirmed, indicators published by SecurityScoreCard provide evidence of the use of compromised JBS credentials of its Australian employees, then traffic to RDP ports in its IP space that didn't belong to known JBS assets.

Reconnaissance of JBS began in February of 2021 followed just one month later by exfiltration of more than 5 TB of data, from March to May 2021. The REvil Ransomware Group armed with the Sodinokibi Ransomware in the breach would later be implicated in the attack. (SecurityScoreCard, 2021)

REDUCING THE NUMBER OF ADMINISTRATORS & PRIVILEGED SERVICE ACCOUNTS

Organizations are attempting to address this challenge by reducing the number of privileged accounts in their Active Directory (AD) environment, and also by reducing the number of service accounts. While this is good cyber hygiene, it doesn't effectively reduce risk.

Identity Risk Management is the proactive elimination of sensitive resources found on endpoints that an adversary uses to live off the land and move laterally. These resources, such as cached credentials, enable adversaries to move deeper into the network in an effort to find what they're ultimately there for. By starving them of their ability to harvest privileged credentials and connection caches, they're unable to move beyond their initial foothold in the network, lowering the mean time to detection (MTTD) and mean time to response (MTTR).

Terence Runge, Chief Information Security Officer (CISO) for Reltio—who also served as Senior Director of Enterprise Security for SalesForce—agrees that these attempts are ineffective. "Reducing the number of administrators and privileged service accounts won't be an effective measure against this problem. Even if you take these measures, IT still has to perform their job function of break-fix issues and other routine care and feeding of endpoints. Additionally, the secure storage of private keys, cached connections, and even users writing passwords into files on their host will continue to be a problem that reducing the number of privileged user and service accounts doesn't address."

Additional risk is caused by:

- hard-coding credentials in Github repos, leading to account takeover of cloud workloads and datastores
- users writing passwords into files on their systems
- developers hard coding credentials in their source code
- users storing precomputed private keys in their home directories—for key-based authentication to services like secure shell (SSH)

IDENTITY AND ACCESS MANAGEMENT (IAM) AND PRIVILEGED ACCOUNT MANAGEMENT (PAM) SOLUTIONS

IDENTITY AND ACCESS MANAGEMENT (IAM) AND PRIVILEGED ACCOUNT MANAGEMENT (PAM) SOLUTIONS

Identity and Access Management (IAM) is a category of solutions that lets users log in to applications and access data without needing elevated privileges. IAM essentially couples authentication (something you know, something you are, something you have) with authorization (something you're allowed to access).

Whereas IAM authenticates and authorizes, PAM limits the number of authenticated and authorized individuals to just the bare minimum number who need access to perform their jobs.

These solutions are failing to eliminate identity risk because they don't eliminate privileged account sprawl. They don't stop problems such as:

- users storing their passwords in files on their systems,
- the necessity for users to have local administrator privileges
- the need for in-app stored credentials
- developers hard-coding credentials or keys in their source code
- users saving connection profiles in apps along with the username/password for the account.

Gary Hayslip, CISO for SoftBank Capital, tried these solutions and saw no measurable decrease in identity risk. "IAM and PAM will perform as described but it won't completely address the problem. IAM and PAM can't see into cached privileged identities, it's typically built for provisioning, and can't support all service account types. Additionally, visibility gaps are typically created by tools since many whitelist privileged account activity. Taking real measurable steps towards managing identity risk can only be done by instrumenting your network with a tool that's continuing to identify and take action on the trail of credentials, kerberoast-able accounts, and connections left cached on hosts and in applications in normal every-day use." Hayslip went on to say that, in addition, the adoption of software-as-a-service (SaaS) solutions creates the potential for what he calls 'shadow SaaS accounts', offering another method of data exfiltration.

RISE OF IDENTITY RISK MANAGEMENT

RISE OF IDENTITY RISK MANAGEMENT

Identity Risk Management (IRM) is a new market of products designed to identify “shadow IT” and other assets that have vulnerabilities affecting the integrity of a network. These assets, especially when unknown to the cybersecurity organization, create identity risk that’s exploitable by adversaries.

Using Illusive’s IRM solution, a company can eradicate three categories of threats facing organizations:

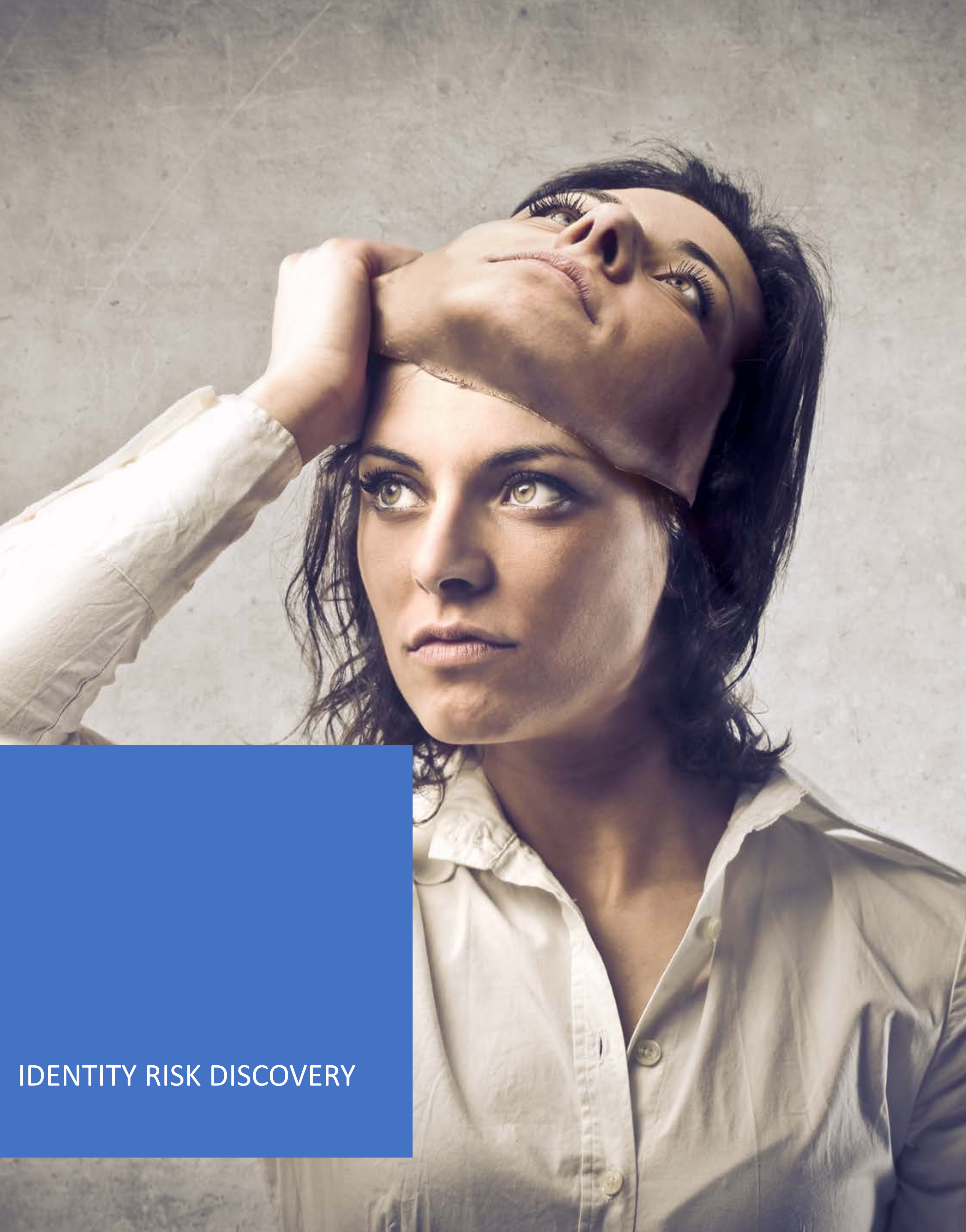
1. Unmanaged identities
    a. Local administrators
    b. Legacy applications and shadow SaaS accounts
    c. Accounts not in MFA/PAM

2. Misconfigurations
    a. Shadow administrators
    b. Kerberoastable services accounts
    c. Identity and password re-use

3. Exploitable identity information
    a. Cached credentials
    b. Stored cloud tokens
    c. In-app stored credentials

By adopting IRM, organizations stop playing “wack-a-mole” with the “bread crumbs” left across endpoints—ones that adversaries use to pivot and escalate privileges once they have a foothold on the network.

Chris Hetner, former security advisor to the chairman of the Securities and Exchange Commission (SEC) and global CISO to GE Capital agrees that IRM is no longer a nice to have. “By reducing your attack surface through IRM, organizations can lower their MTTD/MTTR by eliminating these hidden threats. Instrumenting your network with an IRM solution automates the necessary effort of cleaning up the threats created by privileged account sprawl and cached connections across the network. It’s a critical and necessary approach to creating a hardened security architecture.”



IDENTITY RISK DISCOVERY

Identity Risk Discovery
You can’t treat a risk that you don’t know is there. A solution should identify these identity “breadcrumbs” on the network and clean them up

The recent, highly publicized SolarWinds breach that affected 100 companies happened simply because a highly privileged account password was leaked on the company’s Github repository. This allowed an attacker to change SolarWinds source code and insert a backdoor. Had the company known this credential was leaked and shared between multiple people, it could have quickly addressed the problem by changing the username and password used to access its source code repo.

Identity Policy Violation Mitigation
If you don’t know a set of user credentials is in violation of your security policies, you can’t do anything about it. An IRM solution should be capable of proactively identifying identity policy violations before they are exploited. It should also be able to identify unauthorized connections to your crown jewels, identify risk and unwanted applications on endpoints, and eliminate user credential violations.

In the SolarWinds breach, the company was unaware of the password violation with the account using the weak password “solarwinds123” – an account with access to their source code repository. Later, the Cybersecurity and Infrastructure Security Agency (CISA) announced that the adversaries behind the Solarwinds breach had used brute force attempts (credential stuffing) attacks against victims in order to further compromise more companies, beyond the backdoor they placed into the Solarwinds product.

Protect Privileged Accounts
IRM solutions should be able to use active protection against the abuse of privileged credentials, whether it be user or service accounts, taking active measures against their unauthorized use. Employing active defense measures-–—such as deceptive credentials planted on endpoints and deceptive cached connections—allows organizations to lower the MTTD/MTTR of threat actors who’ve already established a foothold on their network.

Had SolarWinds identified the shared “solarwinds123” account before the actors in the breach, they could have removed the account and instead created individual accounts for those needing access to the source code repository. Further, they could have planted the “solarwinds123” account as deceptive credentials in their environment, then monitored its use to detect attackers.

Recently, an organization with roughly 2,500 employees who deployed IRM identified 1,500 domain administrator credentials, 300 helpdesk administrator credentials, and 220 unauthorized connections to their crown jewels that were cached on endpoint systems. They now have adopted IRM to take proactive measures against identity risk.

An effective approach to IRM should include detection, mitigation, and active defense to ensure that identity risks are proactively identified, cleaned up, then proactively used to deceive adversaries attempting to use them once in the environment. This approach provides an organization an automated approach to continuously cleaning up the environment of identity risk while hunting for threats using these credentials using deception — a lethal three-pronged approach to attack surface management.

PRIVILEGED ACCOUNT MANAGEMENT FAILS: AN EXAMPLE

Many organizations deploy Privileged Account Management (PAM) solutions, thinking this will protect them against virtually all identity risk. Yet in 2010, I worked alongside Mandiant's incident response team in a combined effort with Accenture several month effort responding to an APT group compromise at a large biotech company.

What follows is a step-by-step account of the breach and what tactics, techniques, and procedures (TTPs) were used by the APT actors, plus how the biotech company's PAM solution failed them. (APPENDIX: A)

Reconnaissance

We discovered that the APT group had specifically targeted the biotech company in search of information about its cancer treatment drugs. The initial reconnaissance involved reading press releases on the company's website. The activity had stopped on a press release announcing a partnership with another company—one with which we had established a site-to-site virtual private network (VPN). This was before the concept of "supply chain attacks" really became a common term. We believe they used this information to determine that the best way past our perimeter defense via this supplier.

Exploitation

Several days later, we began seeing in our Security Information and Event Management (SIEM) platform a spike in brute force activity related to legitimate user accounts originating from our supplier's network . The amount of account lockouts that we handled at the helpdesk more than doubled from historical levels, indicating that password spraying was occurring.

Post Exploitation

There was also a rise in the amount of network traffic across our internal core, indicating there had already been unauthorized access established by the APT group . They had successfully moved laterally from our supplier's network into our internal network and were using staging server(s) to copy data in preparation for exfiltration, using password encrypted RAR files as well as outlook PST files.

Despite the fact that we had implemented an enterprise PAM solution-––a leading solution in the market today-––it did not remove cached credentials on endpoints for users that had local administrator privileges, nor did it eliminate cached RDP sessions on hosts that IT used to connect to endpoints for break-fix issues.

Eventually, the lateral movement by the APT group led them to an account with Domain Administrator privileges and access to our Active Directory server, which resulted in them dumping all of the accounts from AD for offline brute forcing. This was a complete compromise of the network, as well as our email server and sensitive data stores, such as servers containing our intellectual property/drug information.

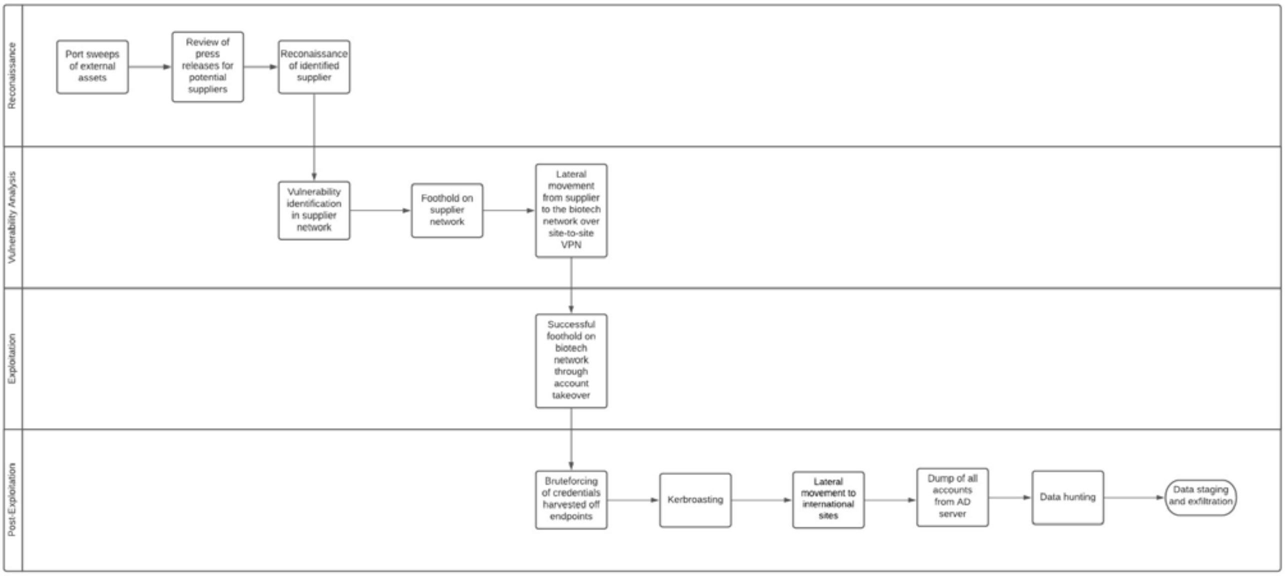
Clearly, hubris and overconfidence in your security controls can lead to a rude awakening.

CONCLUSION

History has taught us over the last two decades how PAM//IAM solutions alone don't prevent lateral movement within a network once a foothold has been established. Credential and connection caching left as breadcrumbs across endpoints in the network are not addressed by these solutions. Only IRM solutions can address this. You can't protect what you don't know you have.

APPENDIX

APPENDIX A: Tactics and techniques used in the biotech compromise


Reconaissance
Port sweeps of external assets
Review of press releases for potential suppliers
Reconaissance of identified supplier
Vulnerability Analysis
Vulnerability identification in supplier network
Foothold on supplier network
Lateral movement from supplier to the biotech network over site-to-site VPN
Exploitation
Successful foothold on biotech network through account takeover
Post-Exploitation
Bruteforcing of credentials harvested off endpoints
Kerbroasting
Lateral movement to international sites
Dump of all accounts from AD server
Data hunting
Data staging and exfiltration

BIBLIOGRAPHY

- 2021 Data Breach Investigations Report | Verizon. Retrieved October 2, 2021, from https://www.verizon.com/business/resources/reports/dbir/

- Kass, H. D. (2021, May 24). Insurer CNA Paid Hackers $40M for Ransomware Decryption. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/cna-payment-40-million-dollars/

- JBS Ransomware Attack Started in March. (2021, November 10). SecurityScorecard. Retrieved February 21, 2022, from https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march

- Explosive Growth of Identities Has Led to a Significant Increase in Identity-Related Breaches. (n.d.) Identity Defined Security Alliance. Retrieved February 21, 2022, from https://www.idsalliance.org/wp-content/uploads/2020/08/IDSA-Infographic-v3-1.pdf

ABOUT KNIGHT INK

Firm Overview

Knight Ink is a content strategy, creation, and influencer marketing agency founded for category leaders and challenger brands in cybersecurity to fill current gaps in content and community management. We help vendors create and distribute their stories to the market in the form of written and visual storytelling drawn from 20+ years of experience working with global brands in cybersecurity. Knight Ink balances pragmatism with thought leadership and community management that amplifies a brand's reach, breeds customer delight and loyalty, and delivers creative experiences in written and visual content in cybersecurity.

Amid a sea of monotony, we help cybersecurity vendors unfurl, ascertain, and unfetter truly distinct positioning that drives accretive growth through amplified reach and customer loyalty using written and visual experiences.

Knight Ink delivers written and visual content through a blue ocean strategy tailored to specific brands. Whether it's a firewall, network threat analytics solutions, endpoint detection and response, or any other technology, every brand must swim out of a red sea of competition clawing at each other for market share using commoditized features. We help our clients navigate to blue ocean where the lowest price or most features don't matter.

We work with our customers to create a content strategy built around their blue ocean then perform the tactical steps necessary to execute on that strategy through the creation of written and visual content assets unique to the company and its story for the individual customer personas created in the strategy setting.

Contact Us

Web: www.knightinkmedia.com
Phone: (702) 637-8297
Address: 1980 Festival Plaza Drive, Suite 300, Las Vegas, NV 89135

ABOUT ILLUSIVE

Firm Overview

Illusive discovers and mitigates privilege identity risk policy violations to disrupt the lateral movement that ransomware and nation-state attackers use to access critical assets. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. Illusive enables organizations to create a hostile environment for attackers by discovering privileged identity risks, mitigating policy violations, leveraging deceptive controls to detect attacker actions associated with identity risk not easily mitigated, and delivering on-demand visibility into nefarious attacker activities.

Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help companies protect their critical assets, including the largest global financials and global pharmaceuticals. Illusive has participated in over 140 red team exercises and has never lost one!

Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com