ARCTIC WOLF

PERSONAL | PREDICTABLE | PROTECTION

2020 SECURITY STRATEGY

PLAYBOOK

CONTENTS

INTRODUCTION

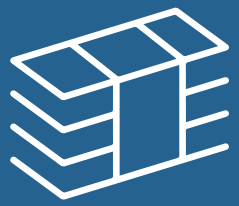
Cybersecurity has undergone a tectonic shift in the past decade.

The threats and challenges organizations face in 2020 have grown tremendously, and organizations must adapt their strategies to defend against much stronger—and better funded—adversaries.

It raises important questions: How do you make sure your security keeps pace with a rapidly changing business environment? What best practices should you follow to defend against today's threats?

We answer these questions—and more—in this security strategy playbook.

6



TRILLION

Cybercrime damages will cost the world $6 trillion annually by 2021. This is up from $3 trillion in 2015.

SOURCE: Cybersecurity Ventures

STAYING AHEAD OF THE CURVE

Monitoring the evolving threat landscape requires constant vigilance. While changing business needs—such as digitization—put new demands on cybersecurity practices, growing threats and the growing attack surface also add new challenges.

To stay ahead in today's environment, while—at the same time—positioning your organization for the future, you need to look beyond buzzwords and understand the desired outcomes of your security strategy.

Bolster Defenses With Hybrid Artificial Intelligence And Machine Learning

The hype around artificial intelligence and machine learning has reached a point where every vendor tries to find ways to eliminate the human element. That's understandable. After all, humans make mistakes and can only solve problems at human speed.

But before you adopt AI-based solutions, it's important to understand the limitations of artificial intelligence and machine learning:

1

Unlike humans, AI can process vast amounts of data fast. However, it's not sophisticated enough and doesn't have the same level of intuition to make decisions that require human intelligence.

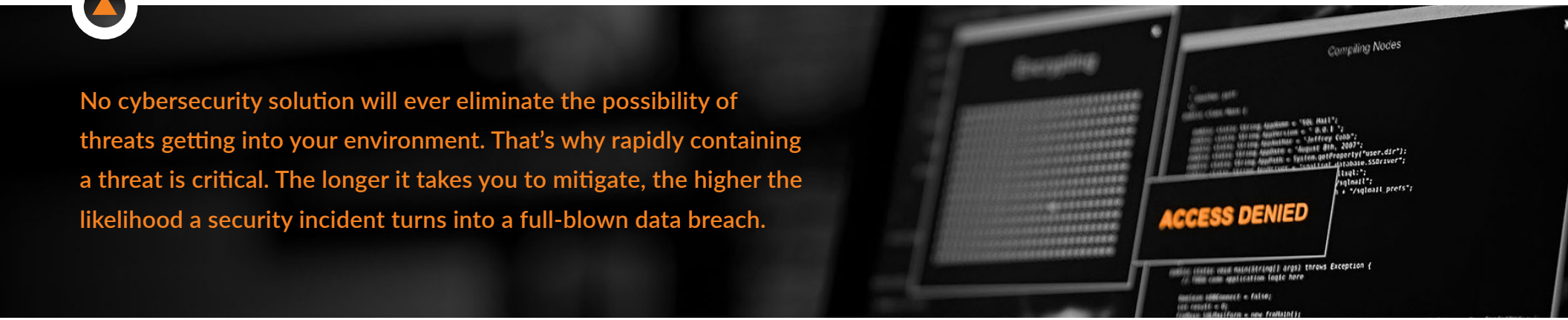
2

AI-driven solutions can identify anomalous patterns to find threats, but there's still the risk of false positives. As a result, you can't rely on AI alone.

3

Since machine learning depends on algorithms, the systems need to be continuously fine-tuned as new threats emerge.

Hybrid artificial intelligence—meaning human-augmented machine learning—combines human intelligence and machine-scale performance. Look for ways to leverage hybrid AI for faster threat detection and response, and for overall improved efficiency.



No cybersecurity solution will ever eliminate the possibility of threats getting into your environment. That's why rapidly containing a threat is critical. The longer it takes you to mitigate, the higher the likelihood a security incident turns into a full-blown data breach.

Close the Visibility Gap with Continuous Risk Assessments

Visibility across the entire environment is a fundamental part of a security strategy—and a constant struggle at the same time. The most effective strategy to eliminate the visibility gap is to conduct risk assessments that identify vulnerabilities and help prioritize mitigation.

- Risk assessments should address not only the technology and the environment (network, devices, etc.), but also your people and processes.
- Since risks change dynamically, perform risk assessments continuously rather than at intermittent intervals.
- To help improve your security posture, risk assessments should include easy-to-consume reports for your key stakeholders and a unified dashboard that consolidates your entire cyber risk.

Go Beyond Vulnerability Management with Rapid Containment

Assessing risks and managing vulnerabilities will help reduce your attack surface. But no cybersecurity solution will ever eliminate the possibility of threats getting into your environment. That's why rapidly containing a threat is critical. The longer it takes you to mitigate, the higher the likelihood a security incident turns into a full-blown data breach.

- Monitor your environment 24x7 using not just technology but also human analysts, so your team can act as soon as it identifies indicators of compromise.
- Implement containment workflows and playbooks to increase the speed and efficiency of your response.
- Block data exfiltration attempts and the spread of malware with host-based containment.

THE FUNDAMENTALS OF CIS CRITICAL SECURITY CONTROLS

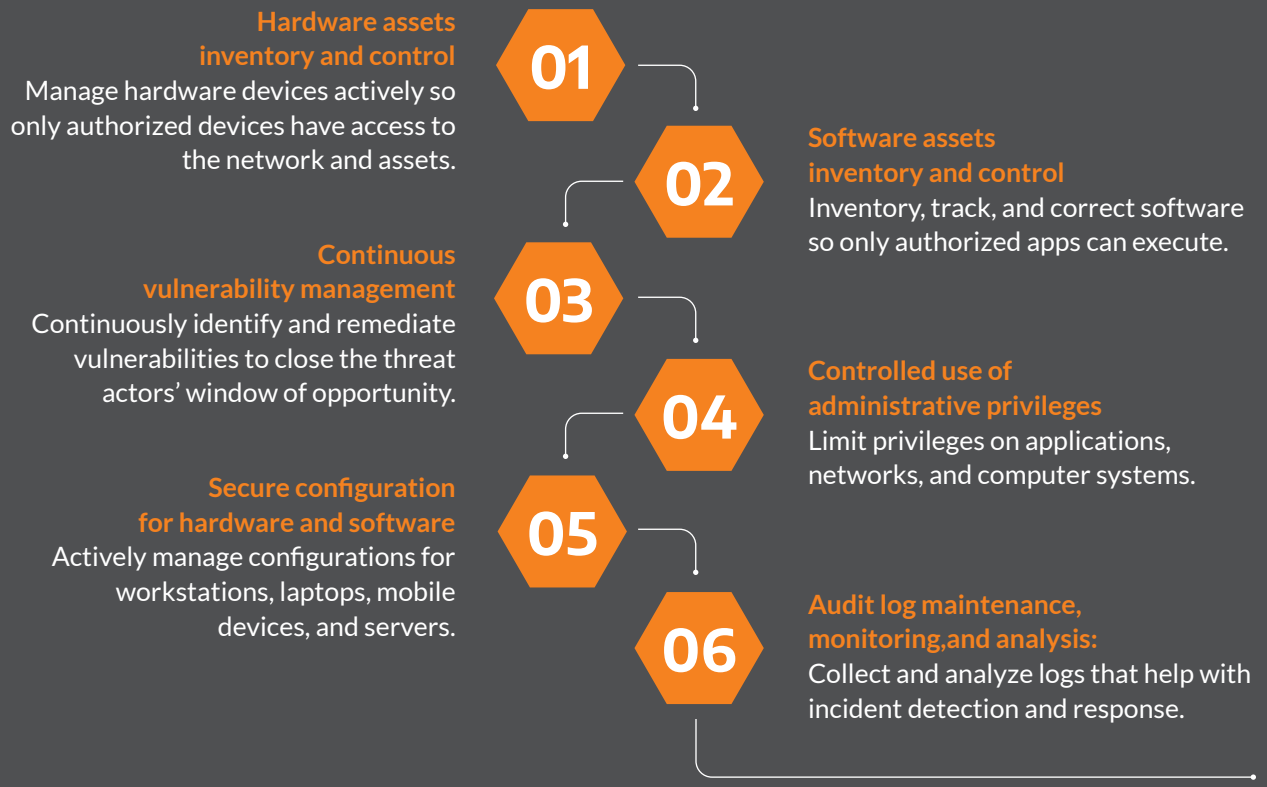
To help organizations develop and prioritize their security strategy, the nonprofit Center for Internet Security has developed the CIS Controls, a set of 20 cyber-defense actions. The controls are derived from common attack patterns and are vetted by a broad community of cybersecurity practitioners, from both the government and private sectors.

Based on cyber defenders' first-hand experience, the controls are regularly updated to reflect new attack patterns. Incorporating the CIS Controls into your strategy ensures you always use the most-effective defenses for the most-common attacks.

The CIS Controls are grouped in three major categories as follows:

1. BASIC

These controls are considered essential, part of basic cyber hygiene, and should be implemented first.



2. FOUNDATIONAL

These controls are based on effective, tried-and-true strategies that provide the greatest reduction of cybersecurity risks.

07 Protection for email and web browsers
Minimize the attack surface for two of the most-common entry points.

08 Malware defenses
Prevent malicious code and files from being installed, executed, and spread through the network.

09 Manage network ports, protocols, and services
Manage vulnerabilities that give attackers entry points.

10 Data recovery
Implement tools, processes, and procedures that enable data-recovery capabilities.

11 Security network device configurations
Establish and manage secure configurations for devices such as routers and firewalls.

12 Defending the boundaries
Control traffic flow through the network to detect, prevent, and correct the flow of data.

13 Data protection
Implement processes and tools that prevent data exfiltration as well as ensure the privacy of sensitive data.

14 Need-to-know access
Control access to critical data and systems based on roles and classifications.

15 Wireless access control
Secure access for wireless local area networks and access points, as well as wireless clients.

16 Account management
Monitor and manage system and application accounts throughout their entire lifecycle.

3. ORGANIZATIONAL

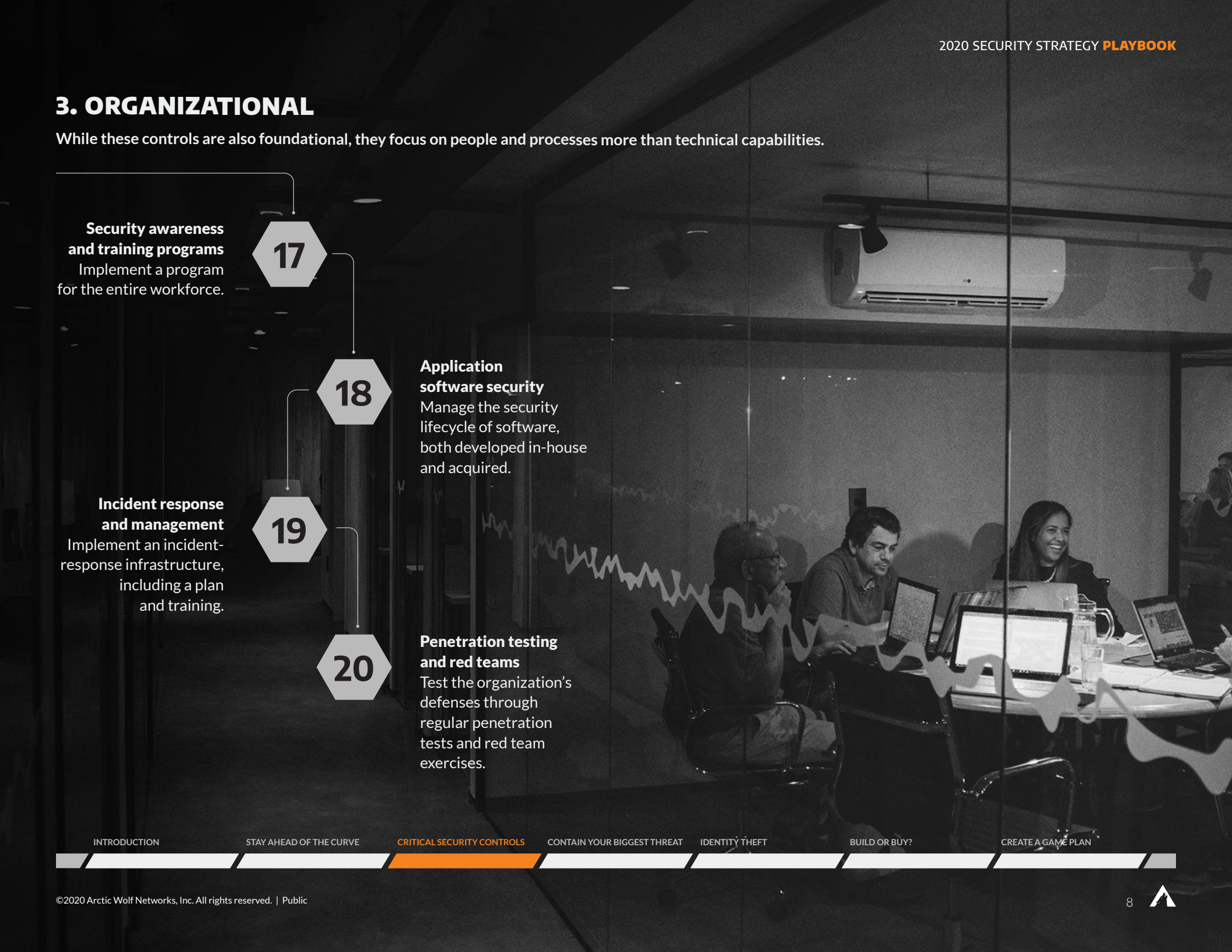
While these controls are also foundational, they focus on people and processes more than technical capabilities.

17 **Security awareness and training programs**
Implement a program for the entire workforce.

18 **Application software security**
Manage the security lifecycle of software, both developed in-house and acquired.

19 **Incident response and management**
Implement an incident-response infrastructure, including a plan and training.

20 **Penetration testing and red teams**
Test the organization's defenses through regular penetration tests and red team exercises.



CONTAIN YOUR BIGGEST THREAT: PEOPLE

People—employees, contractors, and other end-users—will continue to be the biggest threat plaguing organizations in 2020 and beyond. Attackers constantly improve their ability to trick people, and we'll continue to see malware and phishing as the dominant vectors.

End-users make an attractive target not only because their "defenses" are easier to circumvent, but also because compromised user credentials give attackers a more effective way to gain access into your network and systems.

The following best practices will help you contain the people threat in your organization:

Implementation

Implement an ongoing cybersecurity awareness and training program that educates your workforce and other end-users about threats through a variety of activities. Your program needs a consistent cadence to be effective, and should start during the onboarding process for new hires.

Consistent Training

Your IT and security teams are part of the people component—ensure they receive consistent training on the latest threats and defense tactics. If you have a lean team with limited experts in-house, consider engaging an outside firm as an extension of your team.

Analyze Metrics

Use metrics to measure the success of your training programs and identify gaps that remain. Metrics should include both short-term and long-term goals, which help you measure how your security posture improves over time.

People

Make the people component part of your risk assessment and vulnerability scanning. Conduct simulated phishing exercises regularly to test their resilience to phishing scams. Establish a baseline prior to launching an awareness campaign so you can measure its impact.

Security-First

Foster a strong cybersecurity culture that includes a security-first mindset, starting at the top levels of the organization and down to every line employee. All stakeholders should also understand their individual roles in maintaining the security and privacy of your company's assets.

CIS Controls

Refer to the 20 CIS Controls for technical measures that help minimize the attack surface when it comes to your employees, such as limiting access to critical assets based on user roles and managing user accounts through their entire lifecycle.

COMBAT THE RISING THREAT OF IDENTITY THEFT

The heated discussion about deepfakes brings to the forefront the growing concerns over new types of identity theft, such as synthetic identities and account takeover. Both can compromise your organization and are becoming more prevalent.

The threat of account takeover is growing exponentially, considering the billions of stolen user credentials in numerous large data breaches. No matter how well employees are educated, password reuse is a continuing problem. This enables threat actors to use stolen credentials and impersonate legitimate users to gain access to critical systems and data.

Account takeover is often financially motivated, and schemes can lead to significant financial losses. But there are other implications as well, including reputational damage (if attackers take over your social media accounts) and data loss.

The following best practices can help you mitigate the risk of account takeover:

Scan your user data against dark web and grey web sources to identify compromised credentials. Additionally, seek context such as the breach involved. Performing regular scans will help you promptly identify a high-risk situation and prevent a data breach.

Actively manage all user accounts throughout the entire lifecycle. Implement procedures for scenarios such as employees changing roles and requiring fewer access privileges, employees leaving the organization, and completion of DevOps projects that required temporary accounts.

Implement account management procedures that deal with exposed credentials found on the dark web that still belong to active accounts.

Monitor your network and endpoints for unusual user behavior to identify anomalous patterns that may indicate a compromised account.

Educate your workforce about phishing and social engineering scams, and conduct regular awareness activities, including simulated phishing attacks.

Use best practices for password policies, such as changing passwords regularly, and adopt multi-factor authentication.

TO BUILD OR TO BUY?

The most-effective way to coordinate your defenses is by centralizing your security team, processes, and technologies in a security operations center (SOC). A SOC enables you to monitor your environment 24x7 and rapidly respond to incidents. To decide whether you should build a SOC in-house or engage a third-party provider, consider the following advantages and disadvantages of each option.

IN-HOUSE SOC

Pros:

- You have complete control over the technology, processes, and people running the SOC.
- An internal team has deep understanding of your company culture, business needs, and operations.

Cons:

- Finding and retaining talent is a big challenge. With the talent shortage currently estimated at 4 million, employers have to be very competitive to attract top analysts.
- SOCs are expensive to set up, operate, and scale. For small and midsize enterprises, the costs could run into the hundreds of thousands of dollars a year, which is often cost-prohibitive.

The bottom line is that an outsourced SOC has many advantages, but you have to carefully vet vendors and find one who can be a true partner and **provide the outcomes you want.**

SOC-AS-A-SERVICE

Pros:

- It's a cost-effective alternative that saves you money and resources while providing on-demand expertise, so you can continue to use a lean in-house team for more strategic projects.
- SOC-as-a-service vendors typically use best-in-class technology and can easily scale their services to your needs.

Cons:

- Some vendors only offer on-prem or cloud monitoring, but not both, and don't provide 24x7 monitoring by human analysts.
- Not all vendors offer dedicated teams to an organization, and you have to work with analysts who don't understand your business.

CREATE A GAME PLAN

Staying ahead of threats in 2020 and beyond will only get more challenging—and expensive. But you shouldn't compromise your security just because you have budgetary and operational constraints. Bringing in outside resources, as necessary, can help you better align your security strategy with your business needs.

When considering a SOC-as-a-service, seek out a vendor who can provide not only the best technology, but also the personalized service that comes with a dedicated team of analysts and engineers. You need a partner whose value goes beyond cost-savings and provides a holistic approach that helps you improve your security posture.

Protect your organization from cyberattacks and strengthen your security posture with Arctic Wolf. See firsthand how you can stay ahead of the game in today's threat landscape.

ABOUT ARCTIC WOLF

Arctic Wolf Networks delivers personal, predictable protection from cybersecurity threats through an industry-leading security operations center (SOC)-as-a-service. Arctic Wolf™ Managed Detection and Response and Managed Risk services are anchored by the Arctic Wolf Concierge Security™ Team who provide custom threat hunting, alerting, and reporting. Arctic Wolf's purpose-built, cloud-based SOC-as-a-service offers 24x7 monitoring, risk management, threat detection, and response. For more information about Arctic Wolf, visit arcticwolf.com

ARCTIC WOLF

CONTACT US

arcticwolf.com | 1.888.272.8429 | ask@arcticwolf.com
111 West Evelyn Avenue, Suite 115 | Sunnyvale, CA 94086

PERSONAL | PREDICTABLE | PROTECTION

AW_G_Security Strategy Playbook_0320