CYBERSECURITY SERVICES

AVALON

YOUR BATTLE-TESTED, FULL-SERVICE MSSP

Your business, regardless of industry, size, and location, has a unique cyber threat landscape, as well as vulnerabilities that put you at risk of being exploited by these threats. That's why it's crucial to gain awareness of your current cybersecurity posture and consider what you need to do to protect your organization as threats continuously evolve and change.

When you partner with Avalon, you get dedicated access to a hyper-responsive team of cybersecurity professionals who have a constant laser-like focus on your protection. Our deep understanding of governance, security, risk management, and compliance allows us to help you build a highly resilient cyber program, while simultaneously enabling productivity and the continued success of your business.

The men and women who support our managed security services have decades of experience in information security and possess key industry certifications including: CISSP, OSCP, GPEN, CISA, CCNA, CCE, CFCE, EnCE, ACE, GXPN, OSCE, GSEC, ECIH, SSCP, CCSFP, and SEC+. Whether we're conducting a vulnerability assessment, providing security advisory services, or initiating incident response, we provide a five-star experience and unwavering support throughout the engagement.

Avalon is proud to work with clients in industries, including legal, healthcare, manufacturing, education, and insurance and financial services, who seek a greater level of data security.

KNIGHTVISION MXDR

Address blind spots from siloed security solutions and benefit from the most effective means of identifying and mitigating security incidents with Avalon's managed extended detection and response (mXDR) service. KnightVision mXDR is a comprehensive 24/7/365 managed service that collects and correlates data from multiple sources beyond endpoints – email, servers, the cloud, firewalls, network appliances, web apps, and more – and provides detailed visibility in one location to improve efficiency and effectiveness.

KnightVision MXDR includes our world class 24/7 security operations center (SOC), staffed by expert security analysts, who tune, monitor, triage, and respond to security incidents in your environment. The SOC utilizes our SIEM platform to perform advanced analytics and investigate indicators of compromise (IOCs), including malicious entities probing your infrastructure, compromised systems, and potentially unsecured user behaviors.

This combination of people, processes, and technologies delivers round-the-clock threat hunting, monitoring, and analysis across your organization's entire environment, protecting it from the most sophisticated online threats.

What you'll receive from our KnightVision MXDR service:

- Consolidated threat visibility that enables our security analysts to collect and correlate log data across siloed security solutions, reducing blind spots across your organization
- A 24/7/365 SOC that monitors, triages, and respond to security incidents in your environment
- Comprehensive cross-domain threat context and event information throughout the investigation and remediation processes
- Automated alerts and response actions activate workflows that vastly improve SOC efficiency, as well as threat neutralization
- Ongoing tuning via our threat detection and response platform to identify new IOCs
- A security review that includes real-time service health/performance, log analytics, reporting, and recommendations

Why you need KnightVision MXDR

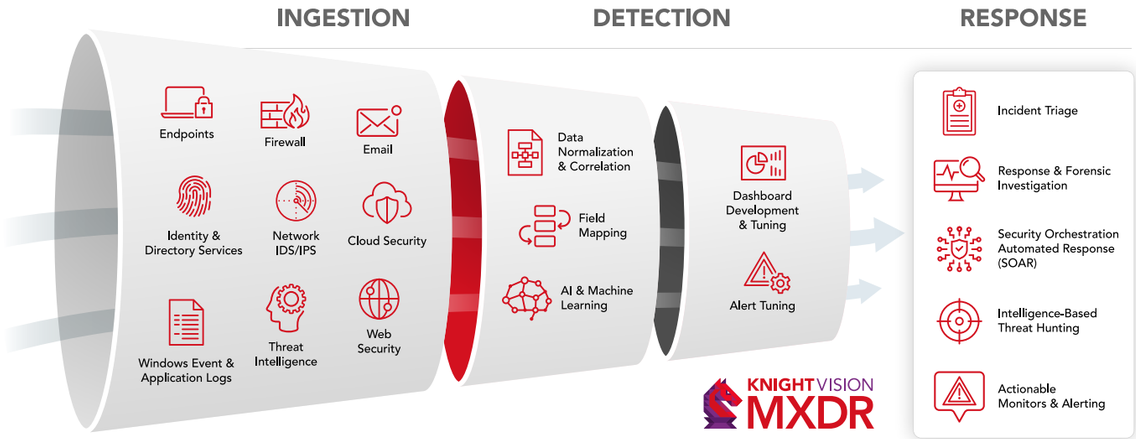
Improved operational efficiency: With the ever-increasing number of threats, there's an ever-increasing number of alerts – and your IT team doesn't have the time to address every one of them. By outsourcing this massive task to Avalon, your IT team can focus on their core duties. Our world-class XDR technology automates many aspects of detection and response, so our battle-tested team is armed and ready to protect your organization, 24/7.

The latest and greatest: MXDR is the best option for stopping threats in their tracks, as you have a team of experts utilizing the most comprehensive range of security telemetry data, including endpoint data, network traffic, and cloud-based environments.

Save time and money: Outsourcing this service to Avalon means you don't have to take on the expense of adding full-time, highly paid security professionals to your payroll. Instead, we become a seamless extension of your IT and security team at a predictable price – minus the costs of recruiting and expensive employee benefits.

How does MXDR work?

XDR technology collects and correlates the data that identifies threats occurring at different layers of your security stack. Our team (who add the "M" to MXDR) can properly configure the XDR to conduct forensic investigation and threat hunting activities across numerous security solutions, all from a single console.



Step 1. Ingest: Data from security log sources such as endpoints, cloud infrastructure, identity solutions, network traffic, and more is brought into the system.

Step 2. Detect: Log data is parsed, normalized, and correlated to automatically detect threats using cutting-edge artificial intelligence and machine learning.

Step 3. Respond: Through human and machine analysis, alerts are prioritized, so our highly trained security analysts and threat hunters can quickly analyze new events and automate investigation and response activities.

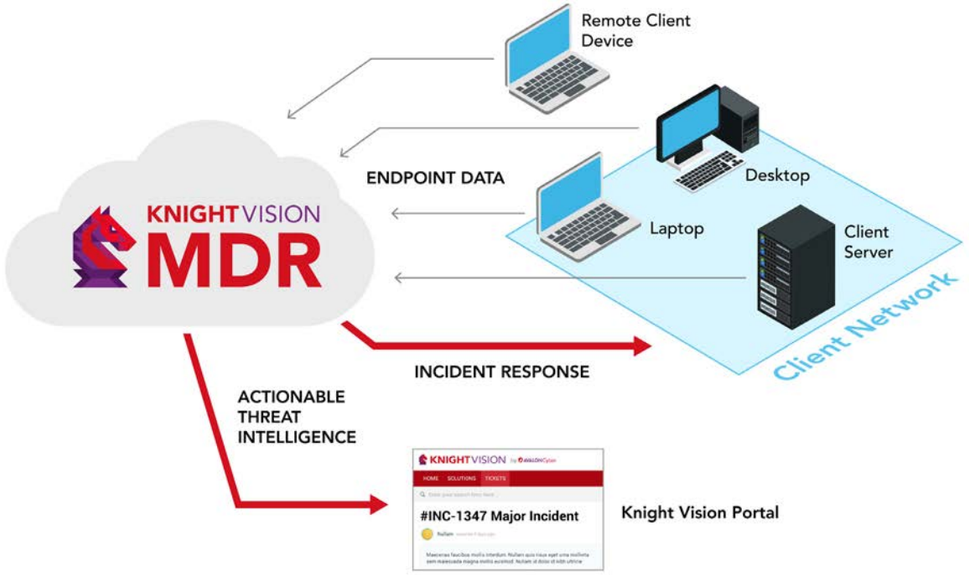
KNIGHTVISION
MDR

Cyberthreats continue to rise in both volume and sophistication. Focusing all efforts on securing the perimeter of your network and relying on antivirus solutions is no longer sufficient. The ability to actively monitor behavioral events at the endpoint level, as well as lateral network activity, is quickly becoming the new standard in cybersecurity.

Avalon's KnightVision MDR service is a robust endpoint monitoring solution that screens malicious behavior at the endpoint level, allowing our team of experts to alert you and take immediate action to shut down a potential threat.

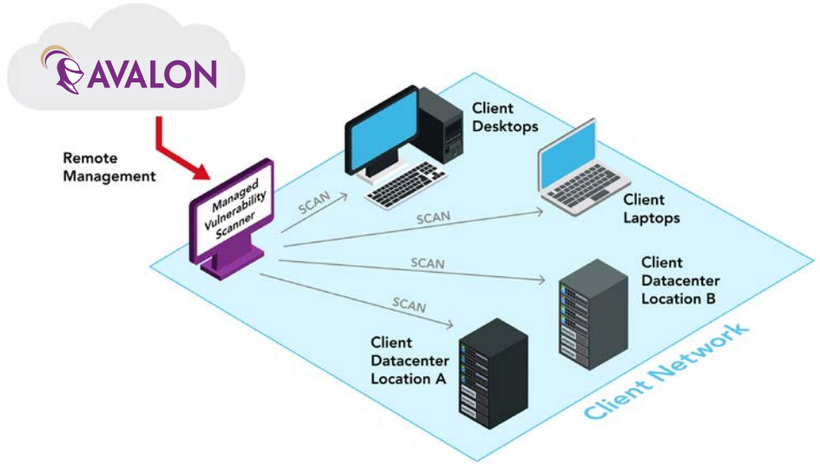
What you'll receive from our KnightVision MDR service:

- 24/7/365 endpoint monitoring by lightweight agents
- Endpoint monitoring inside and outside network
- Remote monitoring
- Behavioral threat detection
- Threat triage



VULNERABILITY ASSESSMENT

Avalon's expert engineers conduct internal and/or external vulnerability scans to identify risks in your company's environment. Our team works with you every step of the way to develop a plan to address the most critical weaknesses and provide insights into the best way to implement improvements.

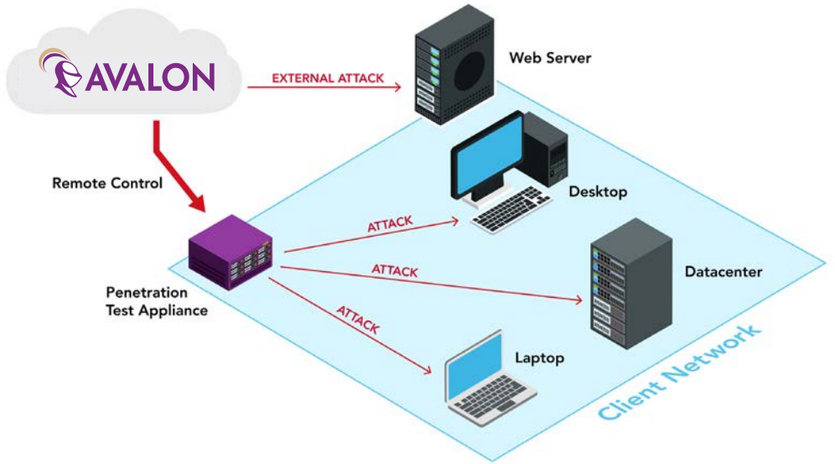


What you'll receive from our KnightVision MDR service:

- A comprehensive scan of all assets within scope (the vulnerability scanning appliance is deployed, configured, and controlled by Avalon experts
- A detailed report outlining critical findings and suggested remediation steps
- A final presentation/executive debriefing of findings, including a Q&A session with your dedicated Avalon technical resource

PENETRATION TESTING

Our cybersecurity professionals safely simulate the actions of a cybercriminal targeting your network by attempting to exploit critical systems to access sensitive data. Penetration testing validates the efficiency of your currently deployed security resources and determines how well employees are following existing security policies.



What you'll receive from our Penetration Testing service:

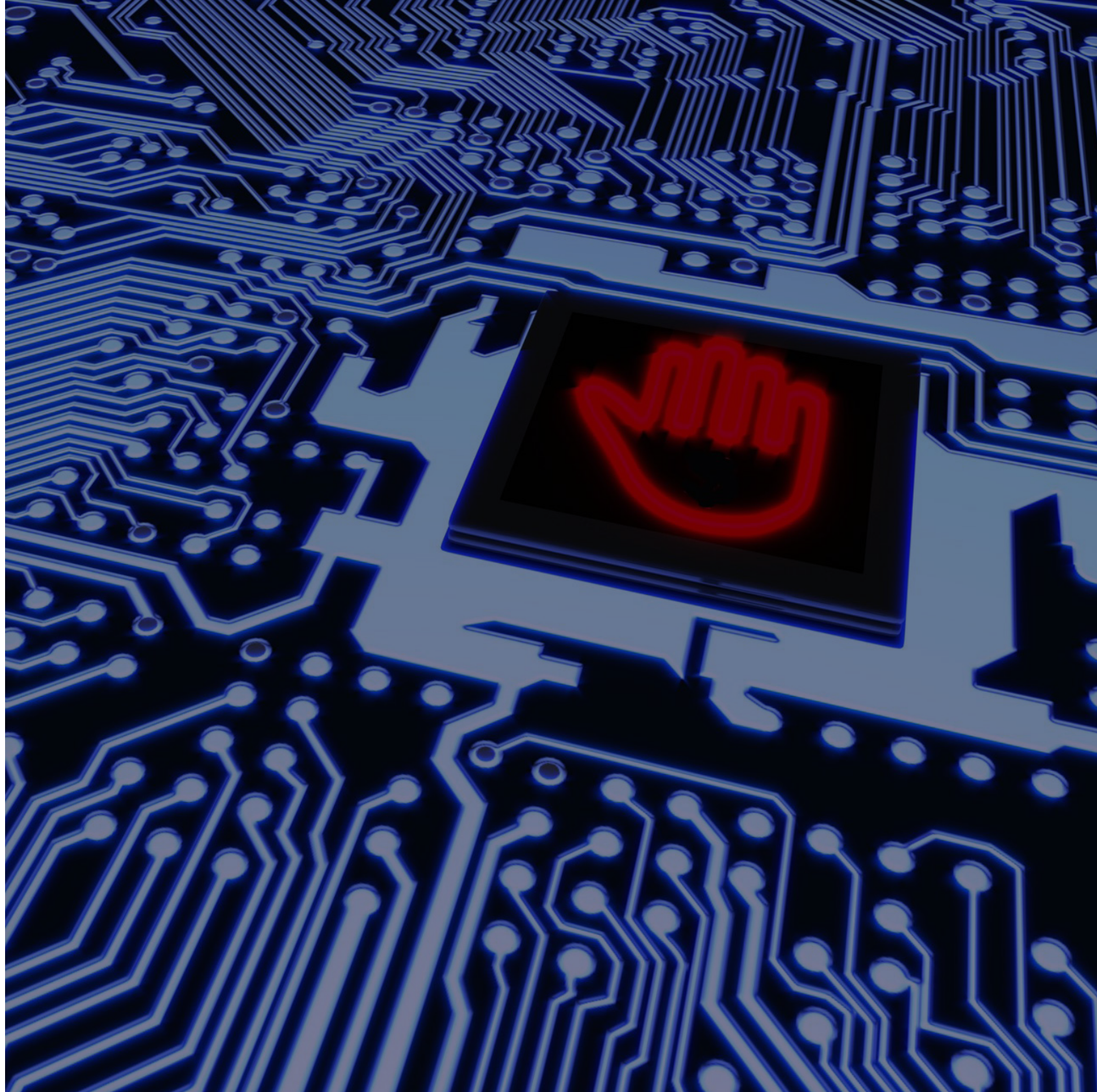
- A test that targets anything with a live IP address (servers, desktops, laptops, firewalls, web servers, and web applications)
- A detailed report outlining critical findings and suggested remediation steps
- A final presentation/executive debriefing of findings, including a Q&A session with your dedicated Avalon technical resource

INCIDENT RESPONSE

If you experience a breach, it's critical that you quickly find and fill the gap in your network and identify what data may have been compromised. This is a true forensic analysis process that traditional IT companies don't necessarily have the capacity for. The Avalon cybersecurity team has extensive experience in digital forensics and technology crime fighting and provides prompt and comprehensive response to cyberattacks. Our experts know where to find critical electronic evidence, and concurrently preserve and analyze it using today's most sophisticated digital forensic techniques and software. We also offer a flexible incident response retainer program that gives you 24/7/365 access to our cybersecurity experts, right when you need them most.

What you'll receive from our Incident Response service:

- Digital forensics and incident response
- Executive debriefing
- Legal counsel support
- Threat hunting
- Actionable threat intelligence
- Comprehensive report detailing results of breach investigation



DATA BREACH REVIEW

Our experts provide data mining and hosting services using industry-leading software, and partner with experienced review teams, if needed. Together, we can help you establish what personally identifiable information (PII) and/or protected health information (PHI) were affected during the cyber incident

What you'll receive from our Data Breach Review service:

- Assistance with culling datasets to make reviews more efficient and cost effective
- Custom layouts to help counsel quickly build entity lists during the review process, so the transition to notification can be completed quickly

DATA BREACH NOTIFICATIONS

We offer secure print and mail services that ensure your confidential documents are processed and delivered promptly, accurately, and with the utmost respect for data privacy.

What you'll receive from our Data Breach Notification service:

- List deduping and data scrubbing to improve data quality
- Full print services and postage consulting
- Record of each document that did not initially reach its recipient

MICROSOFT 365 SECURITY ASSESSMENT

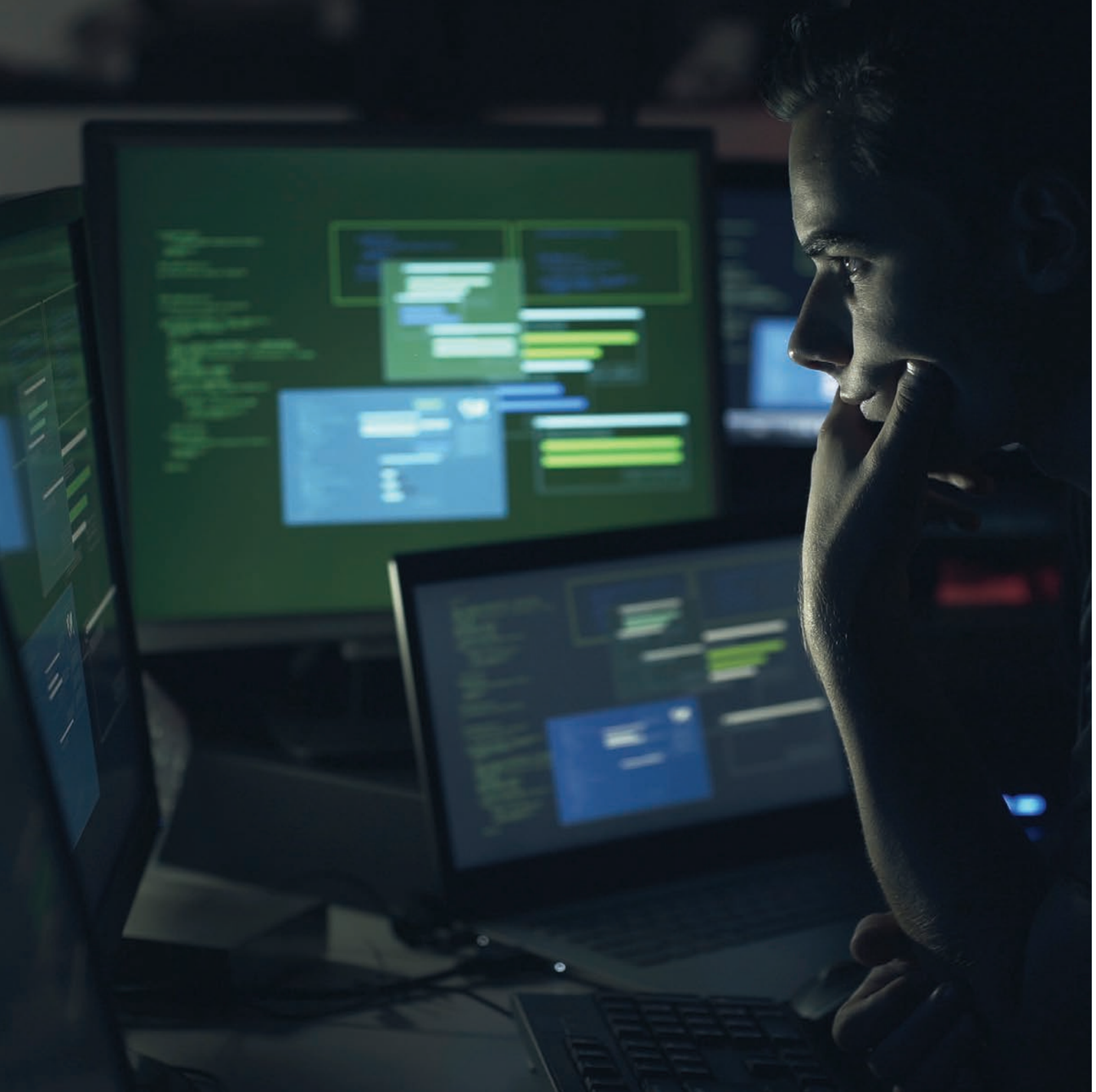
Microsoft 365 offers your team a wealth of tools, but just because your data is in the cloud, doesn't mean it's secure. For example, the default configuration of the tenant likely does not meet security best practices, which could leave your business vulnerable to an attack.

Engaging Avalon to perform a Microsoft 365 best practices security assessment is an easy way to identify areas of risk within the cloud that require attention. Our team will identify any misconfigured settings and provide you with actionable information to remediate those findings.

Our proprietary assessment tool offers checks and testing options modeled after Microsoft and Center for Internet Security (CIS) benchmark recommendations, as well as other security best practices, which results in a more thoughtful and more thorough audit of your environment.

What you'll receive from our Microsoft 365 Security Assessment:

- A combination of manual review and automation to verify relevant settings against known best practices
- A detailed report identifying whether settings pass, fail, or are in a warning state
- Strategic and tactical recommendations that address shortcomings



DARK WEB MONITORING

The dark web is made up of a variety of digital communities, and while there are legitimate purposes for the dark web, it is estimated that over 50 percent of all sites on the dark web today are used for criminal activities, including the disclosure and sale of digital credentials.

To combat this, Avalon offers dark web monitoring and identity theft protection solution with around-the-clock scanning and alerting for compromised data. This sophisticated platform allows your IT team to scour millions of sources, including botnets, criminal chat rooms, malicious websites, and illegal black-market sites – without connecting directly to these risky services.

What you'll receive from our Dark Web Monitoring service:

- 24/7/365 Dark Web monitoring, threat intelligence, and identity monitoring
- Alerts that your digital credentials have been compromised before a breach occurs
- Award-winning, easy-to-use platform that installs in minutes

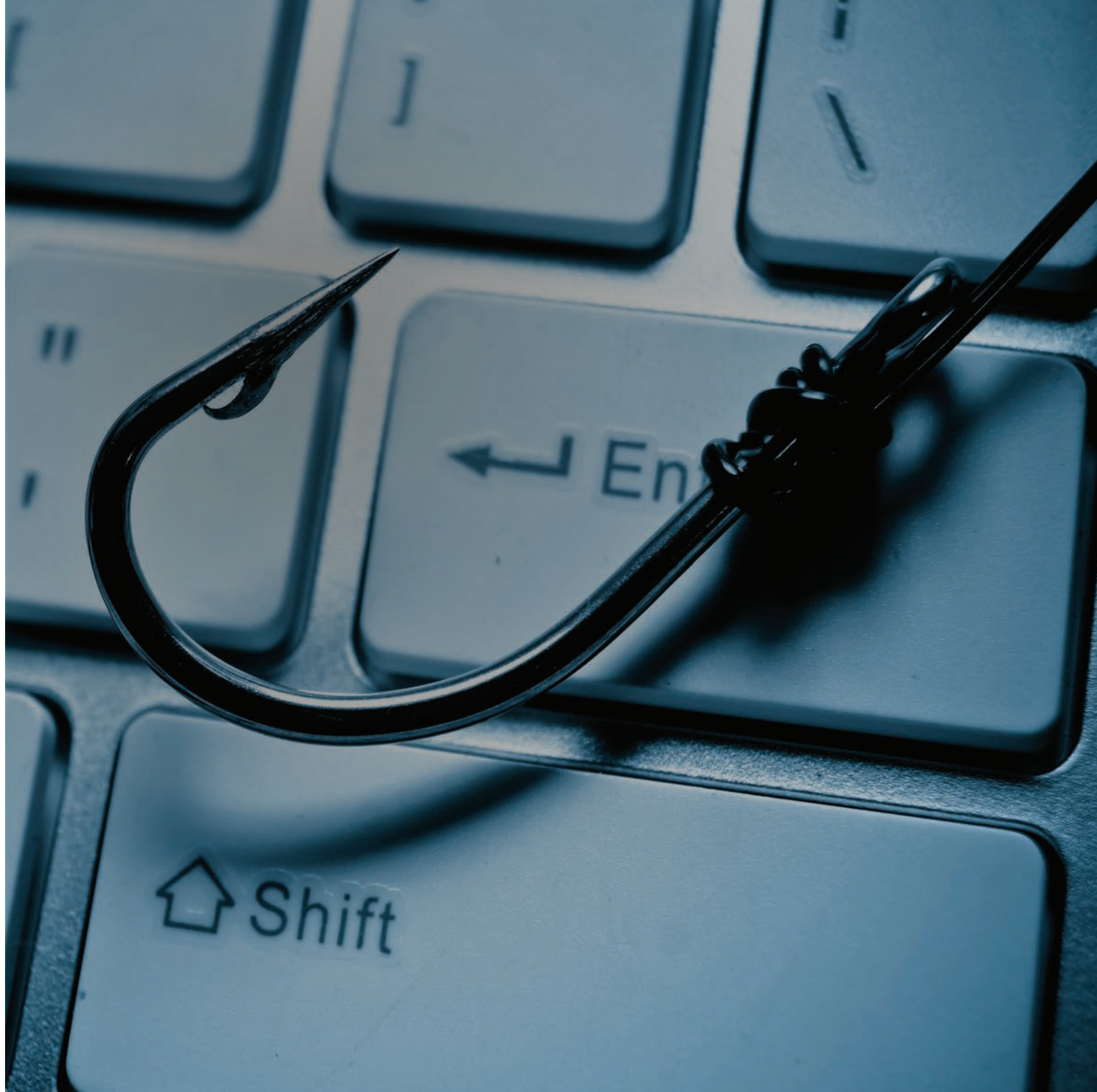
PHISHING SIMULATION AND TRAINING

It's a fact that more than 90 percent of cyberattacks come through phishing emails. While many of your employees may not take the bait on a suspicious email, all you need is one person to click through and you could have a cyberbreach. And with phishing emails becoming more and more sophisticated – and more difficult to recognize – they pose an extraordinary danger to your business.

That's why Avalon offers an innovative program that allows your IT team to launch simulated phishing attacks and run comprehensive security awareness training campaigns to help educate your employees and stakeholders.

What you'll receive from our Phishing Simulation and Training service:

- Access to the world's largest library of security awareness training content including interactive modules, videos, games, posters, and newsletters
- Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates
- Enterprise-grade reporting that shows stats and graphs for both training and phishing



SECURITY ADVISORY SERVICES

Avalon team members are highly experienced cybersecurity strategists, and follow an approach founded in our industry experiences from both commercial and military sectors. We blend practices from Big 4 audit and consulting firms, as well as Department of Defense information assurance programs.

Our deep understanding of governance, risk management, and compliance allow us to help you build a highly resilient cyber program, while simultaneously enabling productivity and the continued success of your business.

REGULATORY COMPLIANCE AND CYBER PROGRAM DESIGN

- National Institute of Standards and Technology (NIST)
  - 800-53
  - 800-171
  - CSF
- DFARS / CMMC
- HIPAA / HITECH / HITRUST
- CIS Top 18
- Federal Banking Regulated Cyber Breach Notification Rule
- NYS DFS Cybersecurity Regulation 23 NYCRR 500
- NYS SHIELD Act
- SEC

STRATEGIC ASSESSMENTS

- Risk Assessments
- SOC 1 & 2 Readiness Assessments
- Gap Assessments & Remediation Services
- Program Development & Enhancement
- Merger & Acquisition Assessments
- Security Awareness Training

INCIDENT RESPONSE EXERCISES

- Guided Incident Response Tabletop Exercises

VIRTUAL CHIEF INFORMATION SECURITY OFFICER (vCISO)

In this type of engagement, Avalon steps into the role of a virtual chief information security officer (vCISO) for companies that do not have the need or means to hire and pay for a full-time resource. Typically, this hybrid approach includes a few hours every month in which our experts become an extension of your team and provide support by overseeing the design, development, and integration of your cybersecurity program

By using a vCISO, you can still meet this common security requirement, take advantage of our guidance and expertise, and save on the hard costs associated with an internal position. We will work with your management team, board, and any additional stakeholders to develop the strategic vision, resources, and protocols required to maintain and mature an appropriate and effective security program for your business.

What you'll receive from our vCISO services:

- Advisement on all forms of cyber risk and plans to address them
- Board, management team, and security team coaching
- Vendor product and service evaluation and selection
- Maturity modeling operations and engineering team processes, capabilities, and skills
- Board and management team briefings and updates
- Operating and capital budget planning and review

Avalon stands ready to assist you with the tools and team required to protect your data – and your reputation – from breaches.

We strive to instill confidence in the members of your company's team, knowing that your approach to cybersecurity will thrive, today and into the future.

If you would like to know more about any of our services, please call us at **877.216.2511** or email **cybersales@teamavalon.com.**

www.teamavalon.com

Avalon Cybersecurity Hotline | 877.216.2511

062425