NASSTAR

CYBER SECURITY AS A SERVICE

AWARD-WINNING, STRAIGHT-TALKING CYBER SECURITY SERVICES

Reducing security risks, improving your resilience and protecting your reputation requires a finely tuned combination of technologies and expertise to cover every corner of your IT estate.

With decades of experience, we've developed a suite of protective technologies, automated monitoring and cyber threat detection tools designed to defend against cyber attacks.

IN THIS GUIDE, WE INTRODUCE YOU TO THE FOLLOWING COMPONENTS OF CYBER SECURITY AS A SERVICE:

THREAT DETECTION AND RESPONSE

Network patrol to isolate threats before they become a problem

SEE IT. STOP IT.

Cyber criminals don't switch off, which means you can't afford to let your guard down at any point. As daunting as it sounds, to defend against these threats, you need to be monitoring your network, services and devices for suspicious activity all of the time.

Try and do it all yourself, and you'll find that it's no simple task, even if you're employing a full-time cyber security expert in your IT team. This sounds exhausting, but it needn't be with Nasstar. We have the technology and the human expertise to keep your organisation safe around the clock.

Our Security Operations Centre (SOC) constantly monitors your infrastructure: network traffic, activity from your applications and services, and activity across employee devices and servers. It's your own technology-led patrol service that means we can identify and isolate threats in near real-time, day or night.

We'll alert you to an attack within 15 minutes and we'll provide a clear pathway to remediation so you can quickly restore working order with minimal disruption.

And because our technology is continually tuned as more data is recorded, it'll keep on getting better with every day you use it.

> *"With over 600 staff, 4,000 students, 1,500 computing and 4,400 mobile devices, our online security is tested on a daily basis, requiring constant analysis against threats and abnormal behaviours. The Nasstar Cyber Security Incident Team offers this additional extended support for us in real-time."*

STEPHEN HARVEY
HEAD OF DIGITAL SERVICES, ARTS UNIVERSITY BOURNEMOUTH

BLOG

COVID-19 the cyber criminals new virus

READ MORE

KEY FEATURES

Patrolling your network against cyber attacks every single day, 24/7

\\ Expansive threat detection

We offer visibility and detection across your entire IT infrastructure using three key telemetry sensors:

- Network Sensor monitors your internal corporate network traffic for known threats as well as any anomalies
- Services Sensor monitors activity from business applications and operational infrastructure, including Office 365, DNS, Active Directory, remote VPN / SSL, web gateways, corporate applications
- Endpoint Sensor is based on software that is hosted on devices such as laptops, desktops and servers. It monitors and detects suspicious or threatening activity, as well as searching for unknown threats and malicious behaviour that don't yet have defined signatures, i.e. zero-day attacks. For the Endpoint Sensor, we can even predetermine automated responses to certain threats to further improve your chances of stopping an attack before it takes hold.

\\ Event use cases

We use 600 pre-defined event use cases, combined with our constantly updated threat intelligence feeds to help us identify potential threat events wherever and whenever they occur. We can also create custom event use cases that are tailored to unique incidents relating to your corporate environment.

\\ Security expertise

As a managed service, you have 24/7 access to our team of highly experienced security specialists. They will be on hand to answer any questions and will continuously monitor your IT environment for known and unknown threats, and suspicious or malicious behaviour.

\\ Reporting

You'll be given access to our online reporting portal, from which you'll be able to view the technical details of every incident flagged. We'll also provide a monthly report to summarise all the events, alarms and incidents that have occurred within your environment, including any remediation recommendations and actions taken.

\\ Near real-time threat response

Using Nasstar's SOC and SIEM, our security analysts are able to identify and isolate threats as they happen – within 15 minutes – ensuring that you don't lose precious time in either mitigating or remediating the threat.

ENDPOINT DETECTION AND RESPONSE

Stop potential incidents in their tracks

PROTECTING YOUR DEVICES AND YOUR USERS, WHEREVER THEY MAY BE

Securing your employees' devices is a cyber security fundamental. But how do you go about this when both devices and people are now out of the office and out of sight?

With more dispersed and flexible workforces than ever before, making sure your devices and users are protected from threats is no mean feat. It requires constant monitoring and immediate action should an issue arise - something that you shouldn't have to worry about.

Our Endpoint Detection and Response (EDR) solution uses the latest software to monitor your endpoint traffic and activity. Laptops, desktops and servers are meticulously scrutinised and analysed by our expert Security Operations Centre (SOC), 24/7/365.

The service proactively searches for malicious behaviour on your devices, automatically stopping any threat in its tracks. This prevents any further harm spreading within your environment, gaining access and control of your data, applications or devices.

With every incident that needs investigating, we'll provide a clear pathway to remediation so employees can quickly get back to work without further interruption. And, because our technology is continually tuned as more data is recorded, it'll keep on improving your cyber immune system and eliminating false positives.

Available as a standalone activity or as a service, you'll only hear from us when there's a genuine concern.

KEY FEATURES

Continuous monitoring of all your devices from advanced threats and malicious behaviour

\\ Expansive threat detection

Many threats can bypass traditional and advanced security solutions in the time it takes for a human to respond to the activity. EDR provides in-depth visibility across all your organisation's endpoints and by automating the response process at this level, you enable:

- Threat detection across the organisation's services and infrastructure
- Automated threat detection and correlation process
- Significantly reduced detection time
- Enabling rapid incident response times
- Prevention of an attack spreading across the rest of the organisation

\\ Visualiser

You'll be given access to the Nasstar Visualiser which will provide you with an overview of all the threats detected on your network, including a log of all incidents and remediation.

\\ Next-level protection

Unlike signature-based security solutions that can be more easily identified, EDR looks for unknown threats and malicious behaviour without a defined signature, providing more protection for your devices, data, and users. If a threat is detected, EDR prevents risks by isolating (automatically or manually) and bypassing attacks from both internal and external sources.

\\ Endpoint Detection Response (EDR) Software installation

Once installed to all your endpoint devices, your agent will continuously monitor using Indicators of Compromise (IoC) to log activity. The automated nature of EDR security allows for:

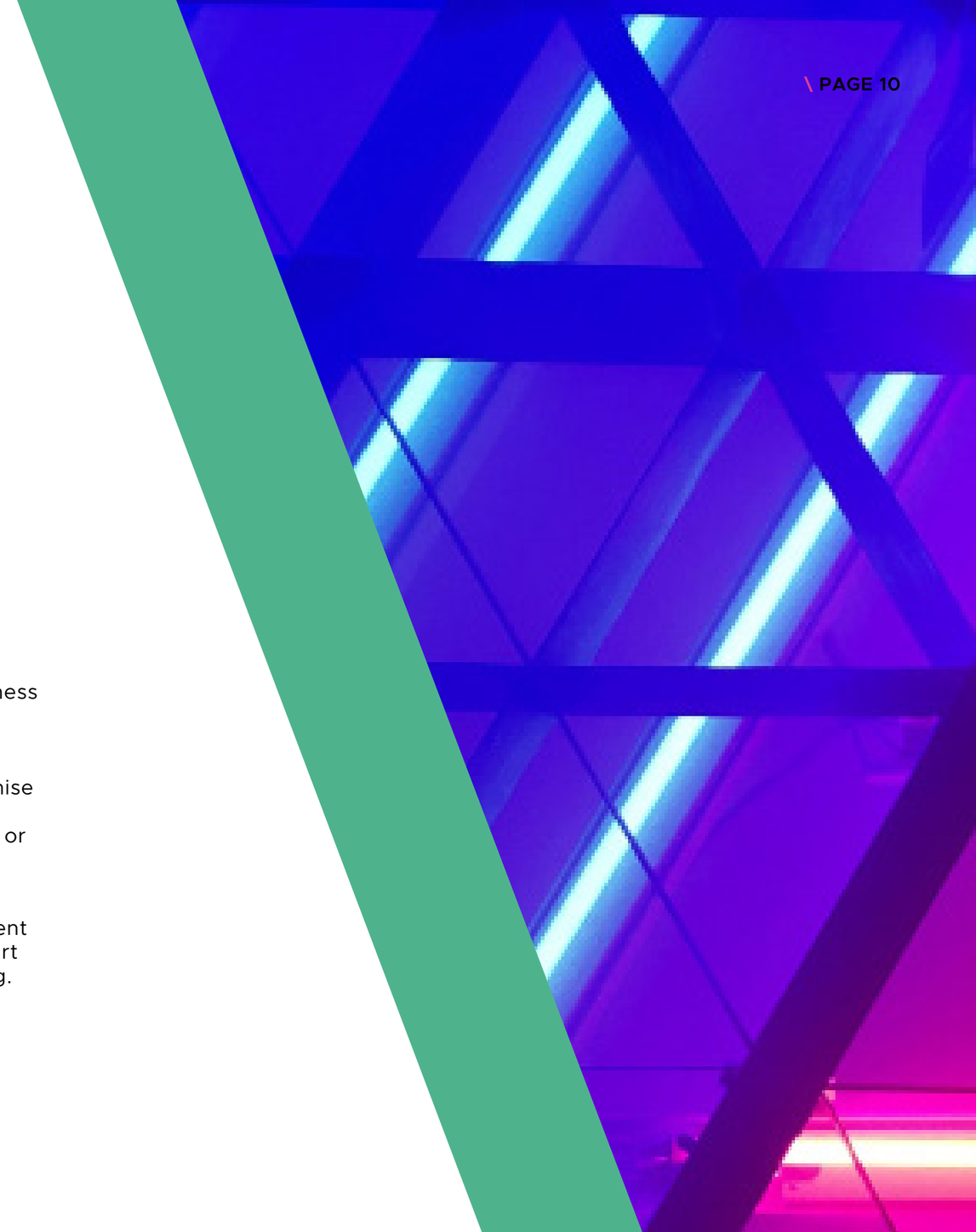
- Streamlined threat detection processing
- Instant threat detection
- Forensic investigation, reporting and response

\\ Incident management and analysis

EDR identifies specific behaviours to alert organisations to potential threats before the attackers can cause harm. If a threat is detected, devices are isolated to prevent the spread of the incident. End-to-end analysis ensures your systems and endpoints are fully scrutinised, and our SOC will co-ordinate with your organisation to mitigate any effects caused.

CYBER SAFETY AND PHISHING AS A SERVICE

Building a more resilient workforce against cyber crime



DON'T CLICK ON THAT LINK...

Over two-thirds of data breaches begin with a phishing email. What was once a high-stakes style of attack reserved for large multinationals and government agencies is now the most common cyber risk to all businesses, whatever your size or sector.

Exploiting "the human factor" cyber attackers' prey on the instincts of curiosity and trust that lead well-intentioned people to click, download, install, open and inadvertently provide access to online and/or financial data.

How to build a human firewall

Too much cyber security education involves generic, one-off sessions – 'telling' people what to do rather than 'testing' their understanding and susceptibility. Our Cyber Safety and Phishing as a Service provides immersive personalised, bite-sized security awareness training, that engages with your workforce to test ongoing knowledge and compliance. Our goal is to help you build a culture in which employees understand how to spot cyber dangers and recognise the value of staying alert. If we're able to make an employee think twice before they open, download or click, we're doing our job.

We value your security. Whether you're a current customer or new to us, our Phishing Risk Assessment is available to you as a standalone service or as part of our broader Cyber Security as a Service offering.

KEY FEATURES

Building a human line of defence against breaches

\\ Expert Training

We establish your staff's existing knowledge, confidence and risk perception levels and provide personalised training, security advice and updates based on each user's knowledge and confidence. Our people-focused security awareness training and phishing platform provides access to:

- An extensive library of cyber awareness training courses, advice and news
- Phishing campaigns at an agreed frequency

\\ Assessment

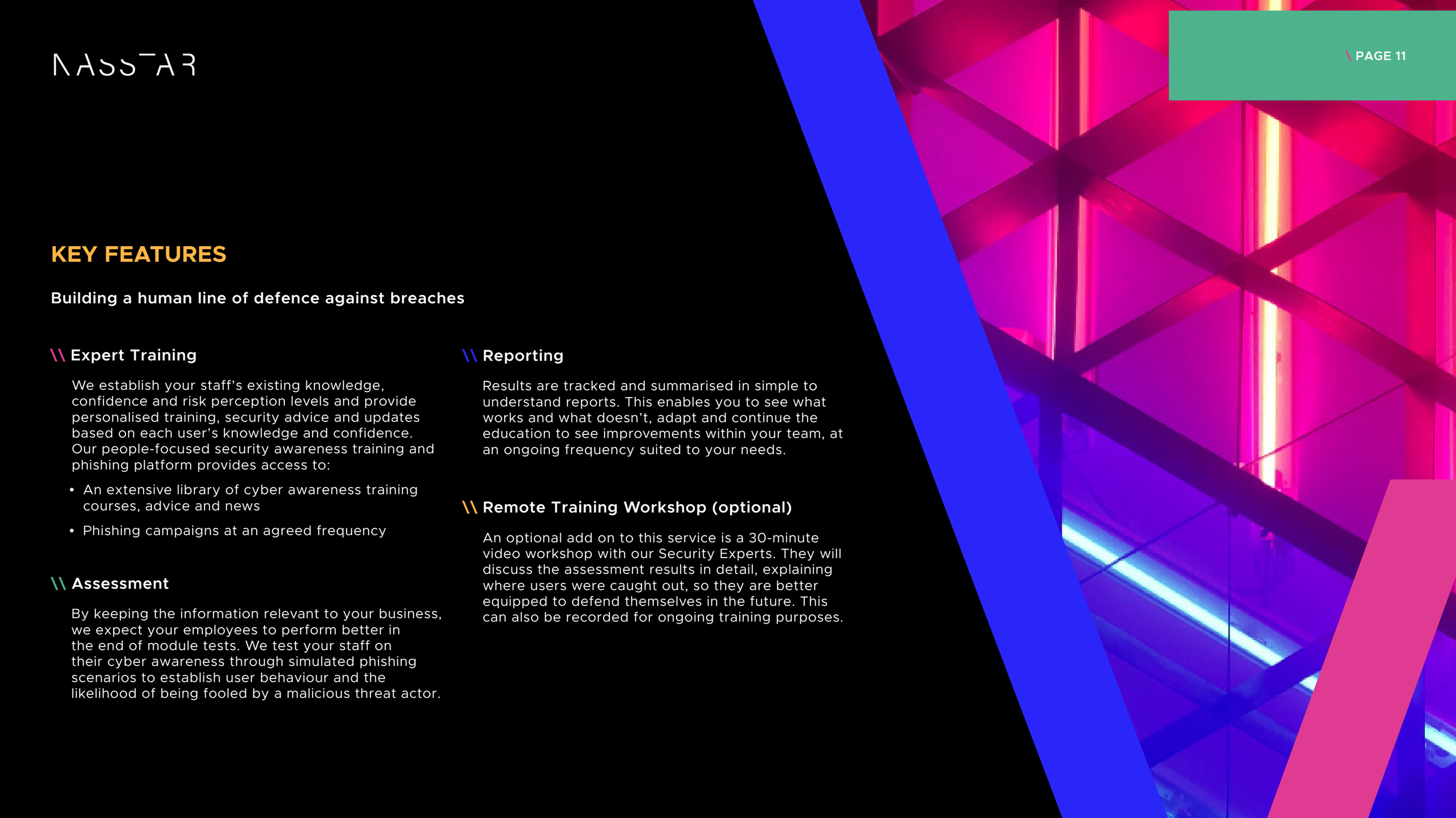
By keeping the information relevant to your business, we expect your employees to perform better in the end of module tests. We test your staff on their cyber awareness through simulated phishing scenarios to establish user behaviour and the likelihood of being fooled by a malicious threat actor.

\\ Reporting

Results are tracked and summarised in simple to understand reports. This enables you to see what works and what doesn't, adapt and continue the education to see improvements within your team, at an ongoing frequency suited to your needs.

\\ Remote Training Workshop (optional)

An optional add on to this service is a 30-minute video workshop with our Security Experts. They will discuss the assessment results in detail, explaining where users were caught out, so they are better equipped to defend themselves in the future. This can also be recorded for ongoing training purposes.



DARK WEB MONITORING

Providing the tools & expertise to stay ahead of cyber criminals

Cyber-crime is a business, not a hobby. In the deep depths, within the hidden recesses of the internet – known as the dark web – there's a vast and lucrative trade in sensitive company and customer data.

SCOURING THE HIDDEN INTERNET FOR YOUR COMPROMISED DATA.

Today, it's not enough for cyber criminals to just steal your data. Without a market for selling your data, security attacks would most likely cease to exist. But there is a market. The exchange of data for money almost always takes place on a hidden part of the internet known as the dark web.

This data can be used by unscrupulous third parties in a myriad of ways. Authentic login credentials can be deployed to access your network; employee records can be used to launch phishing and ransomware attacks; credit card and corporate account details can cost you a fortune before you even know it.

Whether you've suffered a breach or want to keep a precautionary watch on the dark web, you need a way to do this quickly and securely.

Our monitoring engine continuously scans millions of dark web pages and hundreds of dumpsites, using specific search terms provided by you to identify when your data appears or is shared by criminals, alerting you in real-time as soon as a possible breach is spotted. Not only does this help you to take a proactive approach to securing your networks, but you're also one step ahead of criminals looking to exploit the data and do further damage to your business.

You can use our Dark Web Monitoring Service to compliment your existing network security defences, keeping watch 'outside the firewall' provides peace of mind that your company and customer data won't be exploited or fall foul of increasingly stringent data regulations.

> *There are two types of companies; those that have been hacked, and those that will be.*
>
> **ROBERT MUELLER**
> EX-DIRECTOR OF THE FBI

KEY FEATURES

Mitigate risk and minimise loss by keeping a constant eye on dark web activity

\\ Data capture

We capture all new posts made on the dark web as soon they're uploaded, making plain text copies and saving them to a secure database. We create search criteria based on your company-specific data, continuously comparing new posts against the pre-configured custom search terms provided by you.

\\ Continuous Scanning

Our monitoring tools constantly crawl and scrape the dark web, prioritising the hundreds of thousands of sites and forums that are commonly used by cybercriminals to advertise and sell stolen data.

\\ Alerting and reporting

To provide you with the most accurate details of where your data could be exchanged in the dark web, we cover the following types of alerts:

- Historical
- Domain Names
- IP Addresses
- Financial Information

If our systems detect a new post matching your search criteria, an alert is generated in real time and sent to you so you can analyse the details. Our Security Operations team will also receive the alert, and subsequently provide you with a report, including details of possible remediation actions that you can take.

\\ Data Sources

The service provides coverage across a variety of websites grouped into six individual data source components:

- Dark Web: TOR (.onion) marketplaces and sites
- IRC: Internet Relay Chatrooms
- Bins: Anonymous text dump sites used for leaking and marketing data
- Derived Sources: Unlisted and private dumpsites
- Curated Sources: Content from hard-to-reach sites gathered by our analyst team
- Data Dumps: Credentials from large data breaches
- Forums: Hacker forums

VULNERABILITY MANAGEMENT

> *With the increase of digital and cyber-security threats, it has never been more important for effective security monitoring and response. As our trusted partner, and not just a supplier, I feel safe in the knowledge that Nasstar is the best-fit to assist Thrive on our digital transformation journey.*

JOHN STENTON
IT MANAGER, THRIVE HOMES

NOTHING LEFT UNSECURED...

Vulnerabilities exist all over your IT infrastructure – including your endpoints; laptops, desktops and servers - and cyber criminals never stop looking for them.

To stay ahead of the hackers, you need to be on the lookout for these vulnerabilities as soon as they emerge. It is arduous, time-consuming and it never ends. Let Nasstar handle it for you.

Our Endpoint Vulnerability Management Service continuously monitors your entire IT infrastructure – including internal and external networks and connected devices, services and applications. If we spot any weaknesses, we'll tell you how to resolve them.

We even provide a Vulnerability Patch Management service on endpoints that will automatically scan for vulnerabilities and if any are found we will deploy these patches across your endpoint estate, without you having to lift a finger.

FEEL SECURE WITH NASSTAR

Understanding cyber threats is part of our DNA

Certified Penetration Tester

Cyber Essentials Plus solutions

ISO 27001, 20000, 14001 and 9001 certified

SC Awards Europe 2020: Winner: 'Best Managed Security Service'

Finalist: 'Best SME Security Solution'

Finalist: in 'Best Incident Response Solution'

IASME Governance/ Accredited

REQUEST A FREE CONSULTATION

Whatever your size, setup and security training needs, our team can take care of it. With more than 90% of breaches beginning with an email-based threat, it's more important than ever to ensure your employees are cyber aware and can spot malicious behaviour before they cost you your business and reputation.

If you would like to book a complimentary consultation or find out more, please contact enquiries@nasstar.com or call 0345 003 0000.

CONTACT US NOW

nasstar.com

0345 003 0000
enquiries@nasstar.com