VIEWDECK CONSULTING

CYBER SECURITY AS A SERVICE

A complete Cyber Security solution that meets your business needs.

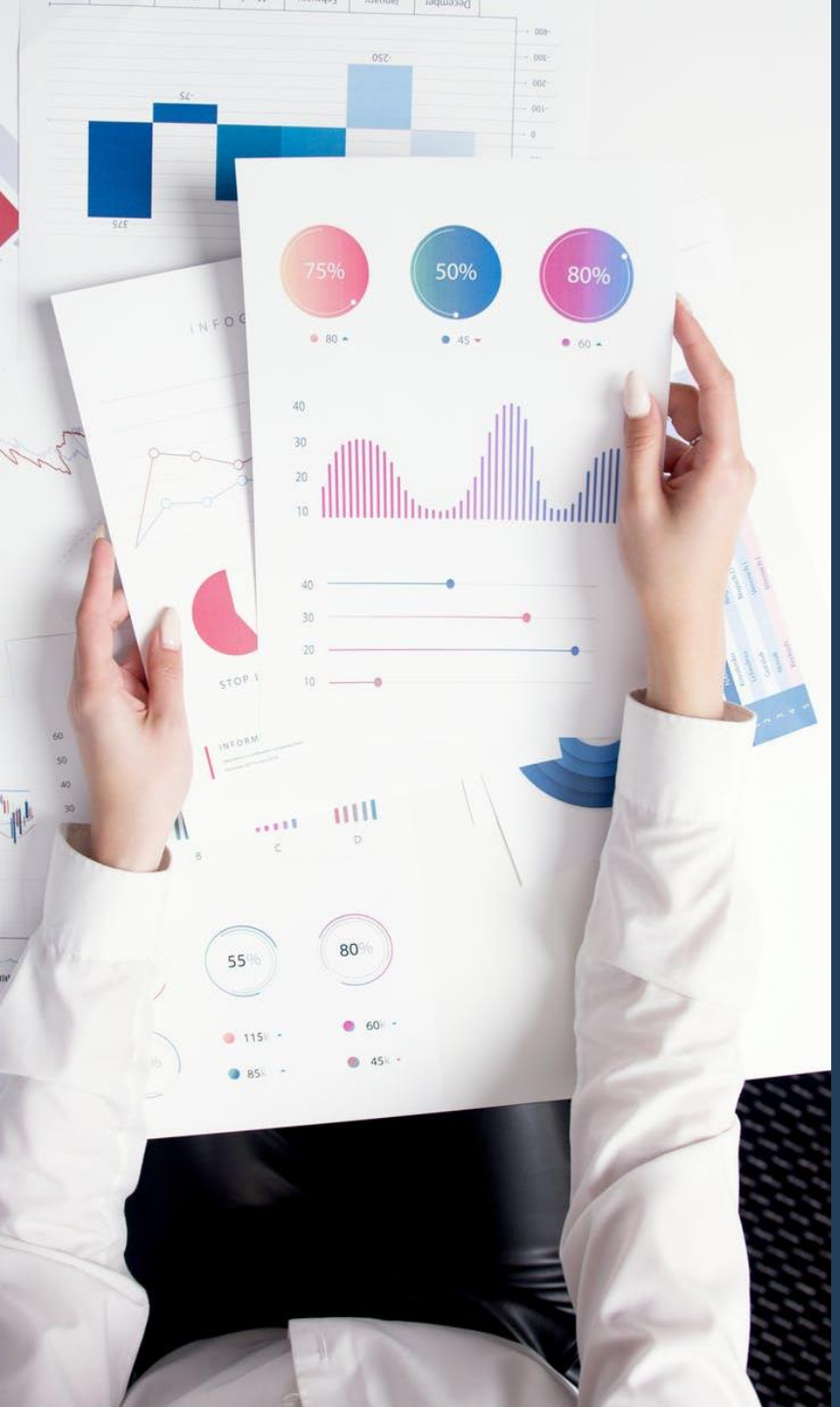
Viewdeck

Driving Secure Digital Transformation

ABOUT US

Viewdeck is an experienced solution and professional services provider, supporting complex ICT change and transformation across the Public and Private sector for over 20 years. Our team comprises of security cleared independent practitioners and associates with real experience from both the UK and overseas. We regularly work in secure sectors supporting UK critical national infrastructure, providing point skills and resources as well as teams supporting some of the largest ICT programmes.

The success of our Security Operation projects has enabled us to develop more services to suit all organisations



CYBER SECURITY STATISTICS

Official statistics from HMG 2020 identified that almost half of businesses (46%) reported having a security breach in the past 12 months.

Of these 46% of businesses, more are now experiencing regular issues at least once a week (32% in 2020 compared to 22% in 2017).

The nature of incidents that organisations are now facing are in 2 main categories; phishing attacks (72%) and viruses or other malware (33%).

Of the 46% of businesses that have identified a breach or attack, 1 in 5 (19%) have experienced a material outcome, losing money or data.

Losing data does not only impact your business' reputation, but it can also lead to fines. Under GDPR, a less severe infringement could result in a fine of up to £10 million or 2% of annual revenue. A more severe infringement could result in a fine of up to £20 million or 4% of annual revenue (whichever amount is higher).

As a business, over 90% of our clients that either use our Cyber Security as a Service or have a continuous Security Project running have been subject to a Cyber Security incident (including both minor and major). 95% of these agreed they should have had some form of Cyber Security protection before the incidents took place. Having Cyber Security protection would have minimised both the financial impact as well as downtime they experienced from the attack(s).

WHAT DOES CYBER SECURITY AS A SERVICE PROVIDE?

Here are the most important features of our Cyber Security as a Service and how they will work for you;

- Daily monitoring of your environment, including; users, emails etc.
- Defence against malicious/suspicious (phishing/spam) emails
- A dedicated team of Cyber Security Specialists
- Notifications through Viewdeck's Cyber Threat Intelligence platforms
- Monthly vulnerability assessments
- Regular Security Operations Reporting
- Annual internal vulnerability assessment
- Up to 24/7/365 service coverage

WHAT TOOLS/SERVICES/APPLICATIONS WILL WE USE TO MONITOR AND REMEDIATE?

- Microsoft Cloud App Security (MCAS): *Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats.*
- Microsoft Office 365 Security Centre: *Allows you to view the security health of your organisation, act to configure devices, users, and apps, and get alerts for suspicious activity.*
- Microsoft Office 365 Security and Compliance Centre: *Designed to help you manage compliance features across Office 365 for your organisation. Links to existing SharePoint and Exchange compliance features bring together compliance capabilities across Office 365.*
- Azure Active Directory (including Sign-in and Audit Logs): *Monitoring of Azure Active Directory sign-in logs and audit logs allow our security analysts to identify patterns of activity, both genuine and suspicious and use the alerts created in MCAS to locate and remediate threats. This includes suspicious sign-ins (we can see in detail the type of login, including location, source IP, user agent, application etc.) and suspicious audit logs (such as modifying user details, escalating privileges, modifying permissions etc.).*
- Microsoft 365 Defender (formerly known as Microsoft Threat Protection): *Is a unified pre- and post-breach enterprise defence suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.*
- Microsoft Defender for Identity (formerly known as Azure Advanced Threat Protection): *A cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organisation.*

WHAT TOOLS/SERVICES/APPLICATIONS WILL WE USE TO MONITOR AND REMEDIATE?

- Microsoft Defender for Endpoint (formerly known as Microsoft Defender Advanced Threat Protection): *Is a holistic, cloud delivered endpoint security solution that includes risk-based vulnerability management and assessment, attack surface reduction, behavioural based and cloud-powered next generation protection, endpoint detection and response (EDR), automatic investigation and remediation, managed hunting services, rich APIs, and unified security management.*
- Microsoft Defender for Office 365 (formerly known as Office 365 Advanced Threat Protection): *Safeguards your organisation against malicious threats posed by email messages, links (URLs), and collaboration tools. Defender for Office 365 includes: Threat protection policies, Reports, Threat investigation and response capabilities, Automated investigation and response capabilities.*
- Azure Security Center: *A tool for security posture management and threat protection. It's integrated with Azure Defender, Security Center protects workloads running in Azure, on-premises and in other clouds. The service enables continuous assessment of security posture, protects against cyberattacks using Microsoft threat intelligence and streamlines security management with integrated controls.*
- A SIEM Solution can be created using Microsoft Azure Sentinel (allowing a greater data ingest of firewall logs, system logs etc. for analysis by our security analysts): *Azure Sentinel is a cloud-native security information and event management (SIEM) platform that uses built-in AI to help analyse large volumes of data across an enterprise. Azure Sentinel provides intelligent security analytics across your enterprise. The data for this analysis is stored in an Azure Monitor Log Analytics workspace. Azure Sentinel is billed based on the volume of data ingested for analysis in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace.*

WHO HAVE WE WORKED WITH IN THE PAST?

Throughout our 20+ years of being in service, we have been able to develop relationships with some of the most exclusive and technically demanding organisations in the United Kingdom.

We have been able to do this because of our security clearance, ISO 27001K certification and Cyber Essentials Plus. We demonstrate persistence to supplying a secure confidential service to all our customers.

Viewdeck

Driving Secure Digital Transformation

CASE STUDY

CASE STUDY: CYBER SECURITY AS A SERVICE

On a recent CSaaS operation, we worked with a global organisation with over 60 offices worldwide on a cloud and security transformation project, we migrated all of their infrastructure from on-premise to Azure, we replicated services, moved data and provided secure operational infrastructure hosted in the cloud.

Throughout the project we upgraded all user licences to A5/E5 which gave 100% security coverage on all accounts. From upgrading licences, we were able to observe, detect and protect all accounts using the security tooling available from Microsoft.

During this period, we identified numerous compromised accounts, which we subsequently secured and continued to monitor to look for any further Indications of Compromise (IoCs). We located points of weakness such as legacy authentication protocols, misconfigured service accounts with elevated permissions, unsecure blob storage locations, administrative accounts being used as service accounts, users accessing restricted data storage areas etc. All issues were resolved with co-operation from their IT department to plug vulnerabilities we identified.

Throughout the ongoing security monitoring, we utilised Microsoft Cloud App Security and built custom policies enabling us to track events that occurred against the user accounts, allowing us to locate targeted accounts, find Indications of Attack (IoAs), locate suspicious activity, locate Indications of Compromise, such as logins from other countries, devices etc.

CASE STUDY: CYBER SECURITY AS A SERVICE

With the capability to identify these threats, combined with the expert knowledge from our security analysts, we transformed their security posture and defended their environment.

As part of the project, a complete ITHC was required which included performing external vulnerability assessments against every external facing IP addresses across their global estate (200+ IP addresses), this provided the organisation with a full report on their external security posture where we identified vulnerabilities, as well providing them with a prioritised list of actions and what vulnerabilities to address first, as well as the accompanying remedial actions to patch the vulnerabilities.

Using Microsoft's Security and Compliance Centre, we responded to numerous reports of phishing and spam emails and performed remedial actions, this included locating the email, deleting the email from recipient's mailboxes, figuring out if anyone had clicked on the URL within the email, locate the hash of any attachments (which alongside Microsoft Defender for Endpoint allowed us to locate if anyone had downloaded the attachment) and perform remedial work from the findings.

Within Microsoft Security and Compliance Centre, we configured anti-phishing, anti-spam, anti-malware, Safe Links, Safe Attachment policies to further secure their environment and for security policies to scan all incoming emails to defend their environment with all available security features that Microsoft offer.

VIEWDECK CONSULTING LIMITED

3RD FLOOR, 207 REGENT STREET
LONDON, W1B 3HH

W: WWW.VIEWDECK.COM
E: INFO@VIEWDECK.COM
T: +44(0) 203 384 3350
F: +44(0) 207 990 9455