Modux Limited

Company Overview & Services

modux

Modux was founded in 2008, initially delivering research, development, and consultancy services within the UK defence sector. Since then, the company has expanded and now employs select security consultants and elite technical experts, each having worked on some of the world's largest digital security and technology programmes. Our combined skill set and collective experience enable us to be both industry leaders and innovators in our fields.

Our senior team come from a Big 4 background, and understand the standard required to deliver to UK industry and HMG. At the same time, Modux is positioned as a specialist cybersecurity boutique, able to respond in a quick and agile way to our clients' needs. We have an incredibly strong Security Consulting skill set and have been responsible for servicing cyber security engagements across both private and government sectors, with extensive experience in the UK across all sectors. This, coupled with our in-house research and software development skills uniquely positions us to deliver this Scope of Work both with high value and quality expertise.

Across telecommunications, finance, defence, rail and aerospace sectors, the team has worked on critical security projects ranging from Critical National Infrastructure to global organisations. We are a NCSC approved CHECK security consulting firm and perform penetration testing and security assurance services that are best in class and market leading.

Description of Services

Infrastructure Penetration Test

Technical security assessments against network elements and associated infrastructure ordinarily consist of automated discovery and enumeration phases, followed by manual assessment and verification stages. Services are assessed for vulnerabilities and security misconfigurations that could be potentially be leveraged to cause data loss, damage or disruption across an organisation.

Often low risk security findings can be chained together leading scenarios that allow for data exfiltration or denial of service from the environment. As such Modux perform every assessment based on an understanding of the environment, its day to day uses and the risks that the organisation may face. This helps us fully evaluate the context of any discovered security weaknesses which allows our client organisations to properly digest the risks.

Web and Mobile Application Penetration Testing

Application penetration testing is primarily a technical security assessment of the application which focusses on discovering security misconfigurations and logic flaws in the application and associated services. The majority of the assessment is based around consultants using the application in the same way an end user would, however the primary goal is to assess the application for potentially insecure functionality that could lead to compromise of the application, any associated data or other application users.

Application penetration testing can also include application side configuration review along with assessments of application areas containing custom code or 3rd party connectivity.

Source Code Review

We propose a full security review of application source code. When performed alongside penetration testing, application source code reviews can help to highlight serious security bugs that could potentially prove elusive within the penetration testing window. Throughout the source code review the application will be reviewed to ensure correct implementation of secure code across the following areas:

- Authentication & Authorisation
- Session management
- Input Validation
- Cryptography
- Error Handling
- Business Logic
- Data Store Connections

Build Configuration Review

A complete build review of servers and infrastructure equipment comprises the following phases:

The target hosts will be scanned using automated tools with valid administrator credentials. This allows the scanners to log-on to the servers and run local checks.

Bespoke information gathering tools are run to gather significant amount of information on the operating system build state. Additional manual on-host checks will be made as appropriate.

The information obtained from the on-host assessment will be analysed and compared to best practice guides published by the Centre for Internet Security and any deviations investigated and detailed. Any specific requirements of the build review will also be assessed.

Where cryptographically stored passwords are obtained during the build review, attempts to crack the passwords will be made using dictionaries of common passwords and other types of weak passwords. The objective will be to identify weak passwords, rather than to try and crack all passwords.

Containerised services and VMs will be reviewed through assessment of the configuration files in conjunction with a review of the deployed configuration.

Incident Response & Remediation

The Modux team are experienced in incident response management and technical investigations, and have worked on a number of complex projects for several large companies.

From the technical side, our team are able to investigate external and internal breaches, understanding how the breach occurred, and helping clients to get back to operational business as quickly as possible. Our team have experience working with web server compromises, malware on internal systems, malicious insiders and ransomware.

We have experienced system administrators on the team, and have worked with clients to rebuild their platforms securely to quickly get back to operational capability.

AD Audit

A review of the current Active Directory will be undertaken. This will identify user accounts which are temporary, unused, overly permissive or potentially malicious. An audit will be performed of account password in order to identify weak passwords configured on the domain.

Cloud Architecture Review

An authenticated assessment of the cloud configuration is recommended for cloud deployments.

As it may be possible for cloud infrastructure to be accessed through compromised applications, engineers' laptops, or third-party code, it is important to ensure that the cloud configuration has been securely configured and sufficiently hardened so that it does not allow further assets to be compromised.

A cloud configuration review is highly dependent on the resources and provider in use. However, there are common themes across all environments that inform our testing. Using permissions that grant us an administrator's perspective we will review: User and Service account configuration and privileges, resource access permissions and hardening, network access control lists and firewalling, secret managements and checks for unintended secret disclosure, along with specific tests devised around the specific threats faced by the context of the platform under assessment.

Asset Discovery

Asset discovery exercises typically consist of the recursive use of open-source intelligence (OSINT) techniques. This is where known values linked to the organisation, such a company or domain name, are used with custom and publicly available tools to discover additional resources connected to the organisation. These newly discovered resources, that may include items such as email addresses or IP address ranges, then feed into further rounds of discovery until no further resources are identified.

Often this discovery will identify assets that are no longer in active use but still exposed to the Internet or systems not under the full management of the organisation's IT department (shadow IT). Systems such as these are often not monitored and hardened fully and may present weaknesses that can be used to compromise further assets in the organisation.

MDM Config Review

A Mobile Device Management (MDM) review is a security assessment designed to ensure the configuration deployed to an organisation's mobile devices is secure.

During an MDM configuration review, Modux will evaluate the implemented mobile device management solution from both a technical and practical stand point, using a combination of the most effective tools and manual exploitation techniques. A thorough and meticulous approach to understanding the configuration's security posture in the context of the organisation against current best practice guidelines will be taken.

Detailed remediation findings with both technical and non-technical descriptions will be provided to ensure that hardening measures can be promptly applied and risk fully assessed.

Kubernetes Review

Although Kubernetes configuration is rarely the cause of an initial breach, a secure configuration is a very important factor in limiting the impact of an application or infrastructure breach.

A configuration review of Kubernetes (K8s) can be performed to assist in discovering potential insecure configurations that could be leveraged during a breach. Configuration and applications are deployed to a Kubernetes cluster using declarative configuration files which can also contain configuration elements which can affect the security posture of the infrastructure & applications, both positively or negatively.

Although Kubernetes configuration can be performed through single commands, as it is often used in Devops or CD:CI environments, mostly the configuration is also stored offline within source code repositories. As such, the majority of K8s security assessments will be performed through an assessment of these files.

Office 365 Review

An Office 365 review is a security assessment designed to identify configurations and settings that may leave Office applications and services vulnerable. Modux will review the configuration, comparing it against the industry standard hardening guidelines to ensure a general all round secure configuration. Further manual review will go on to identify high risk configurations that may present a risk above and beyond those addressed through basic hardening examinations.

A detailed writeup of findings and recommended remediations will be provided at a technical level and summarised along with business impacts for a non-technical audience.

Network Device Configuration Review

The configuration of network devices such as routers, switches, firewalls, and access points will be reviewed to identify misconfigurations and missing hardening controls that should be applied in line with industry best practices.

Network device vendors often offer a number of default settings which provide security functions. There will often be many more, however, that should be configured manually to help to secure the network infrastructure. Using a combination of manual review and analysis through automated tools, our review will highlight these areas for hardening and improvements to protect the network from security breaches.

Wi-Fi Review

Modux will perform a site wide Wi-Fi survey and security assessment. We will map the entire floorplan of the site to identify all organisation network access points, SSIDs, wireless network leakage and rogue network access points. Assessments of the security controls on these wireless access points will be performed to identify any misconfigurations that could allow a malicious user to deploy malicious infrastructure in the environment.
Furthermore, using an authorised device, Modux will analyse the connection methods used by the organisation for any configuration weaknesses.
As wireless networks are the primary network access for most employees in modern organisations. The security of these endpoints plays an important role to protect the security of organisation services

Phishing

Our approach focusses on high risk, high impact weaknesses in corporate structure. We select our targets based on multiple indicators, including role within the organisation, and potential system access. This exercise is not designed to expose mistakes made by individuals, but understand deeper organisational processes that should be addressed.
Our social engineering techniques and methodologies are fully tailored to the client organisation and how they interact with the world. During the course of any social engineering assessment, we will usually utilise one or more of the following attack vectors; phishing & spear-phishing, call impersonation & spoofing, on-site assessments and domain spoofing.
Phishing differs from most other technical security assessments as it can be used to assess and inform both technical security practices as well as the behaviour of staff members. This helps to inform new team awareness programmes as well identifying clear gaps where technology can be leveraged to improve security. Amongst our clients we have seen simulated and real attacks stopped by user reports, when other technology controls have failed.
Both real-world adversarial and simulated phishing campaigns will vary based on their end goals. Most people will accept that it is possible to get an email into an inbox and have a user click a link, as a platform it is designed to facilitate communication and sharing. As part of a tailored phishing campaign, it is possible to enumerate the technology stack, security block and detection rules, as well as the user practices and security posture of end user devices.

Red Team Assessment

Through-out the exercise, we will work with your NOC/SOC teams to understand which attacks were identified, and which went under the radar. We record the data from the entire exercise, and using our experience with SOC monitoring platforms, we can advise on the rules and alerts that would have detected our activity, and help to identify gaps in the current systems.

Designed to discover entry points and security weaknesses that can be compounded to leverage control, Modux consultants have assessed the security of some of the world's largest enterprises. Each assessment begins with intelligence gathering at an enterprise, network and personnel level to assess the potential attack surface and possible entry points. Analysis of the information gathered results in a defined scope, from which focused exercises can begin.

Finding routes into systems and networks, and escalating privileges overtime, the assessments are designed to demonstrate the true resilience of the organisations networks to attack and data exfiltration.

modux

Deliverables

In terms of post-testing and incident response, deliverables are usually focused around the following elements:

- Formal Report
- Remediation Action Plan (RAP) Spreadsheet
- Report Washup Call.

Formal Report

On successful completion of the on-site testing phases a clear and concise report will be produced and delivered electronically (a paper copy can be provided at request). The report will include an Executive Summary for a non-technical readership. This will include a high-level management summary that is suitable for a board level audience.

Modux understands the importance of the final report to our customer and, consequently, we put a great deal of effort into accurately and realistically reporting the findings along with descriptions of the likely impact to the business and detailed recommendations and remedial guidance. All security issues and weaknesses will be clearly ranked in a defined order of Critical, High, Medium and Low risk. All vulnerabilities will have associated recommended remediation solutions stated in order to provide the customer with some guidance on controlling security issues.

As a minimum, the report will comprise a number of sections, such as:

- Executive Summary
- Testing Methodologies
- Scope Description
- Vulnerability Results, including
  - Affected components
  - Issue description and impact
  - Proposed solution and recommendations
  - Further information sources, such as CVE reference or vendor URL.
- Appendix (where applicable), including details such as:
- Screenshots
- Raw results.

CVSS vulnerability ratings can be provided where required. Equally, Modux can also work with the end-customer's own vulnerability rating system, if they have one.

Remediation Action Plan (RAP) Spreadsheet

If requested a Remediation Action Plan (RAP) spreadsheet can be provided. These RAP sheets are useful to customers as part of their Remediation Action Plan as it contains all the assessment findings into a single worksheet of a spreadsheet. The RAP sheet will contain all pertinent details for each vulnerability in the order that they are listed within the formal report. However, it will not contain information such as scope details, methodology used and the executive management summary.

Report Washup Call

If requested, a final Report Washup Call can be provided. This can be a useful discussion with the customer and associated 3rd parties to discuss the findings and possible workarounds or remediation that could be implemented. These are usually done as a conference call but can be done as a face-face meeting.

Further Information:

Danny Rigby

Managing Director

contact-gc@modux.co.uk

Sash Rigby

Technical Director

contact-gc@modux.co.uk

modux