Security Enhancements - New Customer Platform

Summary

The New Customer Platform has been redeveloped to offer enhanced user experience and more importantly enhanced security measures built into the system. Whilst both application and system have been redeveloped through secure code, secure development lifecycle and security engineering principals, most of the security enhancements have been applied to the infrastructure.

Insights have embarked on its journey to acquire ISO 27001:2022 accreditation, passing stage 1 May 2023 and scheduled Stage 2 in November 2023

Security Highlights

- ✓ **Zero Trust**
  - Zero Trust is a security framework requiring all users, whether in or outside the Insights network, to be authenticated, authorised, and continuously validated for security configuration and posture before being granted or keeping access to the New Customer Platform
  - A fundamental approach within the ISO 27001 standard control objectives is that of Zero Trust security. Controls include Access control, to establish physical and logical access controls to information and other associated assets. Privileged access rights, to ensure “least privilege” access.
- ✓ **Learner - One Time Token**
  - The One Time Token prevents some forms of identity theft by making sure that a captured email address cannot be used a second time

- ✓ **No Public IP**
    - Insights servers have no direct connection to the internet, providing a perimeter security solution offering protection against security threats from external malicious actors.
- ✓ **Application Load Balancer**
    - The Application Load Balancer delivers internet traffic to the Insights Portal, providing a barrier between the Internet and the servers, only allowing traffic permitted to communicate with the Insights Portal. Application Load Balancer simplifies and improves the security of the Insights Portal, by ensuring that the latest security SSL/TLS ciphers and protocols are always used.
- ✓ **Secure by Design**
    - With the increasing cyber threat that exists in the world the Secure by Design approach is essential. Insights Development Teams own the cyber security risk from concept to production and manage it effectively through the lifecycle.
      This approach leads to the delivery of a secure product through clearer accountability, simplified processes aligned to the delivery strategy, more use of security standards.
- ✓ **System Block Mode**
    - The system blocks all applications and users by default, allowing access only to those specified in the security policies. Security policies are a set of rules that instruct the system who has access to which system resource. These rules establish the permissions for each user, process, and resource.
- ✓ **Separation of Server Roles**
    - Servers have separated roles reducing the impact of any system breach, with any such breach only impacting a single part of the product.

- ✓ **Secure Communication**
    - Encrypting data whilst it is being transferred from one device to provides effective protection against interception of the communication by a third party whilst the data is in transfer.
- ✓ **Rate Limiting**
    - Rate limiting is a strategy for limiting network traffic. It puts a cap on how often someone can repeat an action within a certain timeframe – for instance, trying to log in to an account. Rate limiting can help stop certain kinds of malicious bot activity. It can also reduce strain on web servers, increasing availability.
- ✓ **Block Cross-Site Scripting (XSS)**
    - XSS is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website. Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click. The New Customer Platform blocks this from happening and denying a potential data leak
- ✓ **Block SQL Injection**
    - A code injection technique that could destroy clients, leak client's data. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input. The New Customer Platform blocks this from happening and denying a potential data leak.

Web Application PenTest – March 2023

The New Customer Platform was subjected to an external web application Penetration Test in March 2023 the report found **ZERO** vulnerabilities.

"During the assessment multiple tests were conducted and included – both manual testing and automated scanning. Testing was conducted from black box perspective, and it was not possible to compromise the host within the timeframe of the engagement. No ports or services were exposed to the internet, and it was not possible to reveal any information about the host."

Insights Learning & Development: ISO 27001:2022 Status

During late 2022 early 2023 Insights made the decision to aim for ISO27001 certification and on that basis the 27001:2022 standards was chosen as these are the newer controls. In May 2023 Insights were independently audited to ensure that the Insights policies are aligned to the 27001:2022 standards. The independent auditor confirmed that policies were aligned and happy for Insights to progress to the Stage 2.

On that basis, Insights have made the decision that the sharing of internal policies will no longer be permissible to external third parties.

Insights however will happily share publicly the following documents from the policy suite to confirm Insights alignment to the ISO27001:2022 standards.

- ISMS 27001 2022 Scope Statement
- Statement of Applicability 27001-2022
- Corporate Information Security Policy