**Infrastructure Team Essential Eight assessment**

**Date:** 16/05/2025  
**Conducted by:** Rohan Batra  
**Team Leads Interviewed:** Codey  
**Team:** Blue Team

**Application Control**

|  |  |
| --- | --- |
| **Do you manage which applications can run on servers and endpoints?** | Yeah - all containerised, some do have volumes with write access. |
| **Do you use any tools to block unauthorised software or scripts from executing?** | No - blue team might |
| **Are users restricted from installing their own software?** | Not sure, Cody is a root user, so is data warehouse team lead, team members are non-root users |

**Patch Application**

|  |  |
| --- | --- |
| **Who is responsible for patching third-party software (e.g. Java, Adobe, browsers)?** | Codey started doing some of that for core ubuntu packages. |
| **How often are patches rolled out? (e.g., weekly, monthly)** | Wasn’t actually a key focus, no schedule blue team has a software that gives us update on out of date software |
| **Are any tools used to track or automate application updates?** | To automate, a software from blue team |
| **How quickly do you patch after a vulnerability is announced?** | No |

**Configure Microsoft Office Macros**

|  |  |
| --- | --- |
| **Are Office macros allowed to run on staff machines?** | NA |
| **Is there a policy or technical control to restrict or approve macros?** | NA |
| **Who manages these settings – Infra or another team?** | NA |

**User Application Hardening**

|  |  |
| --- | --- |
| **Are common applications (e.g. web browsers, PDF readers) hardened or configured securely?** | NA – No infrastructure exists to support this. |
| **Are features like Flash, ads, or Java in browsers disabled or restricted?** | NA |
| **Do you apply security baselines to standard applications?** | NA |

**Restrict Administrative Privileges**

|  |  |
| --- | --- |
| **How is admin access granted, reviewed, and revoked?** | Yes |
| **Is there a clear list of who has domain or elevated privileges?** | Yes |
| **Are admin accounts used only for admin tasks (not email or browsing)?** | Yes |

**Patch Operating Systems**

|  |  |
| --- | --- |
| **Who manages OS patching for workstations, servers, or cloud infrastructure?** | Codey – for VMs |
| **What is your patching cycle and how is it enforced?** | We don’t have one yet - might include in the handover plan |
| **Are updates tested before being deployed?** | Yes |
| **Are any legacy or unsupported OS versions still in use?** | Yes |

**Multi-Factor Authentication (MFA)**

|  |  |
| --- | --- |
| **Is MFA enforced for admin accounts and Blue team systems?** | Partly |
| **Who manages MFA enrolment and enforcement?** | NA |
| **Are there any systems or apps that still rely on only password-based login?** | Getting onto the VM. only VMs are still password based. |

**Regular Backups**

|  |  |
| --- | --- |
| **Who is responsible for backups of blue systems and critical apps?** | Codey |
| **Are backups encrypted, stored securely, and tested regularly?** | NA |
| **Can you restore data quickly in case of a ransomware incident?** | NA – would have to be Deakin IT |

**Infrastructure Team – Essential Eight Security Control Assessment Report**

**Executive Summary**

The Infrastructure Team is tasked with managing the underlying systems that power Redback Operations, including VMs, backups, and core OS environments. This assessment reviewed the implementation of the Essential Eight mitigation strategies within the Infrastructure Team’s control. The team demonstrates foundational understanding but lacks defined patching cycles, backup verification, and enforcement mechanisms, limiting maturity across most controls.

**Assessment Summary by Control**

|  |  |  |
| --- | --- | --- |
| **Control Category** | **Observations** | **Maturity** |
| **Application Control** | Containers are in use, but no enforcement of application whitelisting or blocking is in place. | Level 0 |
| **Patch Applications** | No formal patch schedule. Partially relies on Blue Team tools for visibility. | Level 1 |
| **Office Macros** | Not applicable to current infrastructure. No control or policy in place. | Level 0 |
| **User Application Hardening** | No systems in place to support browser or reader hardening. | Level 0 |
| **Restrict Admin Privileges** | Admin privileges are assigned properly and used only for admin tasks. A list of elevated users exists. | Level 1 |
| **Patch Operating Systems** | Patch management is ad hoc and lacks a defined schedule. Some legacy systems still in use. | Level 1 |
| **Multi-Factor Authentication** | MFA partially implemented; VMs still use password-only access. No unified enforcement. | Level 1 |
| **Regular Backups** | Backup responsibilities exist but are not documented, tested, or encrypted. | Level 0 |

**Strengths**

* Role-based access and admin privilege use are properly handled to some extent.
* Awareness of the need for formal patching and backup plans.
* VMs are managed with intent to secure them, though processes are still informal.

**Areas for Improvement**

* Lack of enforced application control leaves endpoints vulnerable.
* Backup strategy is immature, no encryption or testing poses ransomware recovery risk.
* VMs should transition to MFA-based access controls as a priority.
* Legacy systems still being used, high risk without vendor support.

**Recommendations**

* Create a formal **OS patching policy** with severity-based response windows.
* Implement MFA on all infrastructure touchpoints, including VM access.
* Develop and test a **backup and restoration process**, even if basic to ensure minimum resilience.
* Collaborate with the Blue Team to jointly enforce or support application and script control.

**Conclusion**

The Infrastructure Team shows basic awareness of Essential Eight practices but requires formalisation, enforcement, and routine scheduling to progress toward higher maturity levels.