**Blue Team Essential Eight assessment**

**Date:** 16/05/2025  
**Conducted by:** Rohan Batra  
**Team Leads Interviewed:** Robin, Bikendra  
**Team:** Blue Team

**Application Control**

|  |  |
| --- | --- |
| **Do you manage which applications can run on servers and endpoints?** | Yes, Wazuh, ClamAV |
| **Do you use any tools to block unauthorised software or scripts from executing?** | Not rn, just configured to detect not respond. |
| **Are users restricted from installing their own software?** | Docker infrastructure, only certain people can install anything on docker |

**Patch Application**

|  |  |
| --- | --- |
| **Who is responsible for patching third-party software (e.g. Java, Adobe, browsers)?** | Wazuh, clam, everything infra |
| **How often are patches rolled out? (e.g., weekly, monthly)** | Need basis |
| **Are any tools used to track or automate application updates?** | No, all manual |
| **How quickly do you patch after a vulnerability is announced?** | Almost immediately, depending on severity. |

**Configure Microsoft Office Macros**

|  |  |
| --- | --- |
| **Are Office macros allowed to run on staff machines?** | **No** |
| **Is there a policy or technical control to restrict or approve macros?** | **No** |
| **Who manages these settings – Infra or another team?** | Don’t have domain controllers to that |

**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?** | To the docker infrastructure, via ben. Only roles we look after is our statement, based on permissions via entraID based on principle of least privileges. |
| **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?** | Infra |
| **What is your patching cycle and how is it enforced?** | Infra |
| **Are updates tested before being deployed?** | Yes |
| **Are any legacy or unsupported OS versions still in use?** | No |

**Multi-Factor Authentication (MFA)**

|  |  |
| --- | --- |
| **Is MFA enforced for admin accounts and Blue team systems?** | Go through MFA via Microsoft authenticator. All systems |
| **Who manages MFA enrolment and enforcement?** | Third party other than access into wash which is Duo |
| **Are there any systems or apps that still rely on only password-based login?** | **No** |

**Regular Backups**

|  |  |
| --- | --- |
| **Who is responsible for backups of blue systems and critical apps?** | Managed by Infra unless during upgrades |
| **Are backups encrypted, stored securely, and tested regularly?** | Managed by Infra unless during upgrades |
| **Can you restore data quickly in case of a ransomware incident?** | Managed by Infra |

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

**Executive Summary**

The Blue Team at Redback Operations is responsible for managing and monitoring the organisation’s cyber security posture. This assessment was conducted to evaluate the maturity and coverage of the ASD Essential Eight controls within the Blue Team’s scope of responsibility. The team demonstrates strong awareness and implementation of several controls, particularly around identity management, incident response, and privileged access. However, limitations exist due to infrastructure constraints and tool availability.

**Assessment Summary by Control**

|  |  |  |
| --- | --- | --- |
| **Control Category** | **Observations** | **Maturity** |
| **Application Control** | Tools like Wazuh and ClamAV are deployed for detection, not enforcement. Docker access is limited. | Level 1 |
| **Patch Applications** | Patching is reactive and manual; relies on Infra for execution. No automation tools are in use. | Level 1 |
| **Office Macros** | Macros are not in use. No policies or controls exist, but exposure is low. | Level 0 |
| **User Application Hardening** | No infrastructure to support application hardening (e.g. browsers, readers). | Level 0 |
| **Restrict Admin Privileges** | Access is tightly controlled via EntraID. Principle of least privilege is applied well. | Level 2 |
| **Patch Operating Systems** | Managed entirely by Infra. Confirmed that OS patching is active and no legacy systems used. | Level 2 |
| **Multi-Factor Authentication** | MFA is enforced across all Blue Team systems (Microsoft Authenticator and Duo). | Level 2 |
| **Regular Backups** | Delegated to Infra. Blue Team relies on Infra for backup encryption, testing, and recovery. | Level 1 |

**Strengths**

* Strong control over privileged access and MFA enforcement.
* Clear understanding of team boundaries in patching and backup responsibilities.
* Effective use of detection tools within Docker environments.

**Areas for Improvement**

* Transition Wazuh/ClamAV from detection-only to enforcement mode for improved application control.
* Implement basic automation for patching notifications or workflows.
* Collaborate with Infra to establish application hardening baselines (when infra matures).
* Establish policy-level enforcement for macros, even if not currently in use.

**Recommendations**

* Develop a joint patching and backup policy with the Infrastructure Team to clarify execution roles and schedules.
* Request or build limited infrastructure for testing hardened application builds.
* Advocate for shared governance documents to define control ownership and response protocols.

**Conclusion**

The Blue Team shows strong practices in identity and privilege control (these are mostly managed by third party) but requires improved policy enforcement and automation to meet higher Essential Eight maturity levels.