**Infrastructure Team roles and responsibilities audit**

**Section 1: Role Overview**

|  |  |  |
| --- | --- | --- |
| **How would you define your team’s primary mission at Redback Operations?** |  | Data recovery, allowing people to be able to undo things without learning how things work in the background |
| **What are the top 5 responsibilities your team owns that touch on cyber security?** |  | Data recovery |
| **Who on your team is primarily responsible for those activities?** |  | Codey, Kosta Thompson (monitoring) |

**Section 2: Ownership & Boundaries**

|  |  |  |
| --- | --- | --- |
| **Which security responsibilities do you believe your team owns end-to-end? *(E.g. patching, firewall rules, account provisioning, threat detection)*** |  | Enforcing Encryption – enforced HTTPS, Data recovery, Monitoring(storage and data usage) |
| **Which responsibilities do you believe the *other* team owns?** |  | Everything under, secdevops – secure code, |
| **Are there any activities that your team currently performs where ownership is unclear or shared? Please list them.** |  | No |
| **Have there been any past instances where unclear responsibilities led to delays, risks, or duplicated effort?** |  | During monitoring set up |

**Section 3: Escalation & Coordination**

|  |  |  |
| --- | --- | --- |
| **When a cyber security incident or concern arises, what is your escalation process?** |  | Reach out to Ben/Blue Team/ Cyber Leader (No knowledege) |
| **Do you feel that the current communication and coordination with the other team is sufficient in security-related matters? Why or why not?** |  | Robin and Bikendra(blue team leads), to get permission for authentication for email hosting |
| **Are there specific workflows or processes (e.g. patching, incident response) that would benefit from clearer boundaries or a joint ownership model?** |  | A form of recovery (ben’s idea) with data warehouse. |

**Section 4: Governance & Documentation**

|  |  |  |
| --- | --- | --- |
| **Is your team’s cyber security role and scope documented anywhere? If yes, where? If not, do you feel it should be?** |  | Yes, it has been updated at the beginning of the trimester |
| **Are your team members aware of their specific security responsibilities and escalation paths?** |  | No worries – probably message ben |
| **How do you ensure continuity of security tasks during staff leave or handover?** |  | Because no one is using the VMs – No, out of support during that period |

**Section 5: Opportunities & Recommendations**

|  |  |  |
| --- | --- | --- |
| **Are there responsibilities that your team currently holds but you believe should be transferred or jointly managed with the other team?** |  | No |
| **What’s one thing that would help improve clarity of roles between your team and the other team?** |  | A meeting at the beginning of the trimester and a shared story board |
| **Would you support the development of a joint responsibility charter between teams?** |  | Yes |

**Infrastructure Team – Roles & Responsibilities Audit Report**

**Date:** 16/05/2025  
**Conducted by:** Rohan Batra  
**Team Lead Interviewed:** Codey  
**Team:** Infrastructure Team

**Executive Summary**

The Infrastructure Team at Redback Operations plays a foundational role in maintaining system availability and enabling data recovery. This audit focused on clarifying their cyber security responsibilities, evaluating ownership of key tasks, and identifying communication and governance gaps in collaboration with the Blue Team.

**Key Responsibilities Identified**

* Enforcing encryption protocols (e.g., HTTPS).
* Implementing and managing data recovery mechanisms.
* Monitoring storage usage and data activity.
* Supporting the system backbone required for secure operations.

Team members Codey and Kosta Thompson were highlighted as key team members for operational and monitoring tasks.

**Security Ownership and Boundaries**

The team reported clear ownership of infrastructure-layer security tasks, particularly around encryption and monitoring. Security development and secure coding practices (SecDevOps) were explicitly acknowledged as the Blue Team's responsibility.

**Overlap Identified:**  
A minor overlap was noted during the setup of monitoring systems, where roles between teams were unclear. However, no current activities were reported as shared or ambiguous.

**Escalation & Coordination**

Escalation processes are informally handled, typically by reaching out to Ben (Board Member and Mentor) or Blue Team leads (Who also would then reach out to Ben). While the team expressed no significant concerns about communication, instances like email authentication setup required clearer inter-team permissions.

A suggested improvement includes establishing a formal recovery workflow in collaboration with the Blue Team and Cyber Lead, particularly around the data warehouse.

**Governance & Continuity**

* The team’s role is documented, with the last update made at the beginning of the trimester.
* However, there’s uncertainty around role-specific responsibilities and escalation paths among some team members.
* There is **no defined continuity plan** for staff absences due to low VM usage, which poses a potential operational risk.

**Opportunities & Recommendations**

* **Joint Onboarding Meetings:** Holding a session at the beginning of each trimester to clarify responsibilities and align expectations.
* **Shared Communication Tool:** Establishing a central story board or Slack/Teams channel to track shared tasks or handovers.
* **Continuity Plan:** Developing a lightweight continuity plan to ensure basic infrastructure support during team member absence.
* **Support a Joint Charter:** The team is open to formalising shared responsibilities via a joint responsibility charter.

**Conclusion**

The Infrastructure Team demonstrates ownership over core responsibilities and has made efforts to avoid duplication. Formalising escalation processes, introducing continuity strategies, and increasing shared communication with the Blue Team would further enhance operational clarity and security assurance.