**Blue Team roles and roles and responsibility audit**

**Section 1: Role Overview**

|  |  |  |
| --- | --- | --- |
| **How would you define your team’s primary mission at Redback Operations?** |  | Safeguard redback assets |
| **What are the top responsibilities your team owns that touch on cyber security?** |  | Protecting assets (blue team systems, other systems in infra). Identity and access management. Infrastructure management. |
| **Who on your team is primarily responsible for those activities?** |  | Robin, Bikendra |

**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)*** |  | Security incident and event management, IR, threat hunting, MISP research. |
| **Which responsibilities do you believe the *other* team owns? (Infra)** |  | Setting up infra, patching it, maintaining it. |
| **Are there any activities that your team currently performs where ownership is unclear or shared? Please list them.** |  | Colloborating with reverse engine proxies(codey) and securing it with WAF(Robin). Email infrastructure(blue team will hand it to infra). |
| **Have there been any past instances where unclear responsibilities led to delays, risks, or duplicated effort?** |  | Within the team when the trimester started, later on it became a collaboration. During local testing. More defined during production |

**Section 3: Escalation & Coordination**

|  |  |  |
| --- | --- | --- |
| **In case of a cyber security incident or concern arises, what is your escalation process?** |  | NA |
| **Do you feel that the current communication and coordination with the other teams is sufficient in security-related matters? Why or why not?** |  | Very isolated, don’t know much about what is happening in other teams. |
| **Are there specific workflows or processes (e.g. patching, incident response) that would benefit from clearer boundaries or a joint ownership model?** |  | Yeah, if there is a red team. |

**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?** |  | High level yes, not a defined scope . |
| **Are your team members aware of their specific security responsibilities and escalation paths?** |  | Responsibilities – yes, Escalation – No |
| **How do you ensure continuity of security tasks during staff leave or handover?** |  | Documentation and backups |

**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?** |  | Not sure |
| **What’s one thing that would help improve clarity of roles between your team and the other team?** |  | Shared communication channels, a weekly update thing, maybe a main channel. Cyber leader catchups. |
| **Would you support the development of a joint responsibility charter between different teams?** |  | Yes but it would be hard. |

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

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

**Executive Summary**

The Blue Team at Redback Operations is responsible for safeguarding digital assets through proactive security monitoring, incident response, and threat analysis. This audit aimed to clarify their scope, assess role boundaries, and identify coordination opportunities with the Infrastructure Team.

**2. Key Responsibilities Identified**

* Security incident and event management (SIEM).
* Threat hunting and intelligence (including MISP).
* Incident response planning and execution.
* Identity and access management across Redback systems.
* Partial infrastructure collaboration and transition work (e.g. email handover).

Robin and Bikendra lead most security operations, from strategic oversight to hands-on tasks.

**3. Security Ownership and Boundaries**

The Blue Team claimed ownership over high-level cyber security tasks and threat operations, while clearly delineating infrastructure setup and maintenance as the responsibility of the Infrastructure Team.

**Overlap Areas:**

* Collaboration on proxy and WAF configurations with the Infra Team.
* Shared responsibility during email infrastructure setup.
* Some early trimester confusion during local testing saw some duplicated effort and waste of time and resources but was resolved by the time of production rollout.

**4. Escalation & Coordination**

There is currently **no formal escalation pathway**, which poses a risk during active incidents. Team members acknowledged that inter-team coordination is often isolated and lacks regular visibility into the Infrastructure Team’s activities.

Recommendations included establishing shared communication channels and routine cyber leadership syncs.

**5. Governance & Continuity**

* A high-level scope of what the team does exists but lacks detail.
* Team members understand their own responsibilities but are unclear on formal escalation processes.
* Continuity is maintained through internal documentation and backup procedures.

**6. Opportunities & Recommendations**

* **Define Escalation Protocols:** Establishment of clear procedures and contacts for escalating incidents internally and to other teams.
* **Shared Communication Channel:** Create a dedicated Slack/Teams channel or weekly sync between Infra and Blue Team leads.
* **Clarify Shared Tasks:** Defining who leads vs supports tasks like reverse proxy setup, email infra, and WAF configurations.
* **Support a Responsibility Charter:** The team supports developing a joint charter but notes it may require effort and guidance.

**Conclusion**

The Blue Team effectively manages key cyber security tasks but would benefit from structured communication and escalation processes. Increased collaboration with the Infrastructure Team through defined workflows and shared tooling would improve operational efficiency and reduce silos.