Spike Research Report

By Dylan Rodwell: 1053410989

Report Topic: How can user roles and access controls be defined and implemented in the incident response system to ensure secure and efficient management of incidents?

Executive Summary

Incident response systems are used by organisations to mitigate, identify, control and eliminate security breaches and cyber threats. When designing a system like this, the key to ensuring both the security and efficiency of the system is to implement Role Based Access Control (RBAC). Implementing RBAC into this system is a critical step to significantly reduce risks of users exploiting higher levels of access, unauthorised access to sensitive information, and simplifies the administration of users and groups.

This report explores the positive impact of RBAC in an incident response system explores the general concepts, key benefits and best practices of implementing RBAC, and why it is a critical component of tracing internal breaches and identifying and isolating damages.

It is recommended that incident response systems adopt RBAC to predefine user roles that are tailored to specific operational requirements and use the principle of least privilege to prevent users from exploiting higher access than they should have. In addition, scheduled permission reviews, maintained detailed audit trails and regular training should be implemented to ensure ongoing integrity with evolving incident response processes and regulatory requirements.

With the inclusion of these practices, it will significantly reduce the risks of potential security breaches and unauthorised access to sensitive information and systems.

Introduction

RBAC uses a role permission hierarchy system to manage access to certain processes and information, allowing users to be restricted from parts of the organisation they shouldn't have access to. In incident response systems, the ability to separate user groups using different privileges makes internal system tasks like tracing the source of a breach or identifying the scope of an attack more streamlined and efficient, saving valuable time when attempting to control damages of attacks and patch exploited vulnerabilities.

The problem discussed in this report is a lack of standardised role definitions and user access control management can lead to unauthorised access of sensitive information, compromised integrity of incident management, and a reduction of efficiency leading to longer response times. If access is not properly managed, it can be difficult to trace attacks back to it's source, making rapid action difficult and could lead to attacks having a larger scope of damage.

This report looks into the best practices and implementation of RBAC to suit the context of an incident response system. The scope of this report focuses on the internal user management of the response system and does not explore on user management in other parts of the organisation. The goal of this report is to provide recommendations on how to implement RBAC into a response system environment and educate the user on the benefits this will have on the security and user management of the environment.

Research and Exploration

This section reviews common access control models and key approaches to creating a secure and effective system.

Access Control Methods

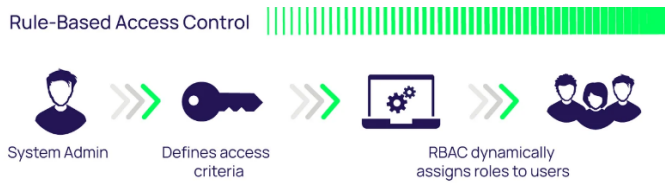
The first method explored is the Role-Based Access Control (RBAC) method. This method focuses on managing privilege for specific roles in an organisation. Users are then assigned to these roles and inherit permissions based on what roles they are assigned. This makes managing the permissions of a large group simpler

Figure 1

The second method discussed is Rule-Based Access Control (RBAC). This method dynamically assigned roles to users based on pre-determined rules and criteria. This method is useful if users should only have certain privileges between certain times of the day, however it is harder to implement than the check boxes that are used for Role-

Based Access Control as the conditions have to be programmed in and it could become complex to tweak if a lot of rules need to be programmed.

Figure 2



Based on these two access control methods, it is recommended that the Role-Based Access Control method be adopted for use in an incident response environment. This is because the incident response system might have multiple teams or multiple teams in multiple groups doing different things and working together, so using group roles it is easier to manage different parts of the team who have different responsibilities. Role based is also the better choice because the main use of rule based is to dynamically change permissions under certain conditions, for example certain hours in the day. If there is a breach outside the scope of those allowed hours this prevents the team to respond immediately and the condition would have to be changed before they can act, losing valuable time and potentially allowing the attack to get worse. The team should have constant access to their privileges so they are always able to monitor, identify and respond to vulnerabilities and attacks in the system.

Technologies and Approaches

This section discusses relevant technologies and how they can help resolve the problem of poor access control.

Access Control

As talked about in the section above, the **Rule-Based Access Control** is the preferred method of access control and is recommended because of it's ease of use and implementation, and effective management of pre-defined teams.

Tools like **Active Directory** make implementing access controls simple and centralised, making it easier to manage and modify privileges of groups.

Authentication Tools

It is important to check the identity of the user who is working under these permissions and verify that it is the correct person to avoid breaches.

Okta Workforce Identity is a tool used by over 14000 global brands (*Top 13 Identity and Access Management Tools|2024 | Zluri*, 2024) that has user authentication and access control capabilities. It uses a variety technology to help manage user identity and permissions, such as:

- Single Sign-On that lets users access multiple applications with a single set of credentials.
- Multifactor Authentication (MFA) that checks if the user has access to different personal platforms such as sms, email and phone call, which verifies their identity.
- User Lifecycle Management that automates the process of giving and removing permissions when an employee joins or leaves the company.

Supporting Practices

Supporting practices that can be introduced to further enhance the monitoring and effectiveness of access control are:

- Just-In-Time(JIT) Access: temporarily elevating user permissions in extreme circumstances to help control a situation as quick as possible.
- MFA: ensuring that the user who was given permissions is the user that is currently using them and that they have not been hacked or infiltrated.
- Audit Recording and Monitoring: keeping logs of all access and actions means it is easier to trace breaches and attacks to the root cause and patch the vulnerability quicker.

Discussion

This report has identified that efficient, secure and rapid action incident response systems rely on structured, secure and flexible access control management. Role-Based Access Control has been identified and recommended as the model to use as it is simple to implement and maintain while also being flexible and its use case aligns with typical incident response team structures.

Using RBAC to manage user group permissions means the principle of least privilege can be used to ensure proper allocation of privileges and prevent unauthorised access or compromising sensitive information.

There are other access control models that can be used in the incident response environment that offer more flexibility. However, the added complexity could prove to cause delays or misconfigurations. If this were to happen in a time-sensitive environment like incident management, it can cause catastrophic problems, which is why the RBAC model is recommended.

Recommendations

The recommendations of this report are clear:

- Implement access control in the incident response system.
- Use the RBAC model to organise team and group permissions.
- Integrate the access controls into a central management system such as Active Directory.
- Implement the principle of least privilege when assigning permissions.
- Enable Just-In-Time Access for emergency privilege escalation.
- Create and maintain a detailed audit of user access and actions.
- Review and update role permissions regularly to ensure it stays up to date with the current needs of the environment.
- Regularly perform role-specific training to keep teams up to date with changing policies and procedures.

Implementation Considerations

Major implementation considerations

- Training
    - Targeted training must be provided to users to keep them up to date with current policies and procedures.
- Role Definitions
    - Parties apart of management should clearly define specific roles and allocate appropriate permissions.
- Tool Integration
    - The incident response system needs to be integrated with the access control and identity management systems.
- Audit and Monitoring
    - Audit logging should capture all logins and actions to maintain a detailed trail for incidents to be traced back to.
- Periodic Access Reviews
    - Reviews of permissions should be performed regularly to verify all permissions are allocated correctly or if it needs modification.

References

- Hoffman, B. (2023). *Access Control: Models and Methods | Types of Access Control*. Delinea.com. https://delinea.com/blog/access-control-models-methods
    - Figure 1 (Hoffman, 2023)
    - Figure 2 (Hoffman, 2023)
- Lindemulder, G., & Kosinski, M. (2024, August 20). What is role-based access control (RBAC)? IBM. https://www.ibm.com/think/topics/rbac
- Stone, M. (2025, January 7). Role Based Access Control Explained: RBAC Security Overview. Concentric AI. https://concentric.ai/how-role-based-access-control-rbac-helps-data-security-governance/
- Why is Role-based Access Control [RBAC] Important for Cybersecurity? - Neumetric. (2024, February 25). Www.neumetric.com. https://www.neumetric.com/role-based-access-control-rbac-for-cybersecurity/
- Top 13 Identity and Access Management Tools|2024 | Zluri. (2024). Zluri.com. https://www.zluri.com/blog/identity-and-access-management-tools

Generative AI Declaration

ChatGPT has been used in this report to help structure the formatting for this report. This includes a description of what structure to use for each section and how to format the report.