Indonesia Jobs Expertini®

Security Operations Engineer

Apply Now

Company: Funding Societies | Modalku Group

Location: Indonesia

Category: other-general

Funding Societies | Modalku is the largest SME digital financing platform in Southeast Asia. We are licensed in Singapore, Indonesia, Thailand, and registered in Malaysia. We are backed by Sequoia India and Softbank Ventures Asia Corp amongst many others and provides business financing to small and medium-sized enterprises (SMEs), which is crowdfunded by individual and institutional investors. And here at Funding Societies | Modalku we live by our core values:

Serve with Obsession: Build win-win relationships for the long-term by having a customer obsession.

Grow Relentlessly: Strive to become our best, most authentic selves.

Enable Teamwork, Disable Politics: Only by forging togetherness, we help each other succeed.

Test Measure Act: Stay curious and reinvent ourselves, through innovation and experimentation.

Focus on Impact: Create impact through bias for action and tangible results.

As a **Security Operations Engineer**, you will lead efforts to identify, analyse, evaluate, and act upon security risks and threats. The Engineer will carry out security threat identification, analysis, and remediation to ensure efficient and timely mitigation of the threats, as well as understand the threats' risks and potential business impacts. The engineer will act as an

incident handler and manage the end-to-end workflow of security incidents based on the defined process. The engineer will also be involved in Splunk Cloud Administration (integrations, use case creation, health check) and the development of the team's processes and continuous service improvement.

Requirements

What will you do:

Incident Response

- Monitor and analyse security alerts and incidents to identify potential threats.
- Investigate security incidents promptly, utilising various tools and technologies.
- Coordinate and execute incident response activities in collaboration with cross-functional teams.
- Contain and mitigate security incidents to minimise impact and prevent further compromise.
- Develop and implement incident response plans to enhance organisational resilience.
- Create incident report in a timely manner for applicable incidents.

Log management and Integrations

- Configure and integrate log sources into splunk cloud and create dashboards for various use cases.
- Develop and maintain log management strategies to ensure the collection and indexing of relevant data.
- Troubleshoot and optimise log sources to enhance data accuracy and completeness.
- Integrate Splunk into the needed log sources, if needed.
- Collaborate with Managed Security Service Provider (MSSP) and other internal security teams to develop and finetune correlation rules and alerts.
- Implement best practices to enhance search and reporting capabilities.

Threat Intelligence

- Stay current with the latest cybersecurity threats and vulnerabilities.
- Review threat intelligence reports and perform the necessary follow-up actions.

Collaboration

- Collaborate with internal teams and external partners to share notable incidents and improvements.
- Participate in cross-functional training exercises and simulations.
- Mentor other team members about Security Operations work.

What we are looking for:

- Strong understanding of behavioural aspects of cybersecurity incidents.
- Excellent interpersonal, communication, and presentation skills.
- Professional working habits and quality-oriented.
- Willing to work with and report under the Security Operations Manager.
- Relevant certifications related to Splunk and Incident Response are a plus.

Benefits

- Time off - We would love you to take time off to rest and rejuvenate. We offer flexible paid vacations as well as many other observed holidays by country. We also like to have our people take a day off for special days like birthdays and work anniversaries.
- Flexible Working - We believe in giving back the control of work & life to our people. We trust our people and love to provide the space to accommodate each and everyone's working style and personal life.
- Medical Benefits - We offer health insurance coverage for our employees and dependents. Our people focus on our mission knowing we have their back for their loved ones too.

Mental Health and Wellness - We understand that our team productivity is directly linked to our mental and physical health. Hence we have Wellness Wednesdays and we engage partners to provide well-being coaching. And we have our Great FSMK Workout sessions too to keep everyone healthy and fit!

Learning & Development: We believe learning should never end and we support everyone with curated learning programs on our internal learning platform

Tech Support - We provide a company laptop for our employees and the best possible support for the right equipment/tools to enable high productivity

Apply Now

Cross References and Citations:

1. **Security Operations Engineer Jobs Indonesia ↗**
2. **Security Operations Engineer Jobs Indonesia ↗**
3. **Security Operations Engineer Jobs Indonesia ↗**
4. **Security Operations Engineer Jobs Indonesia ↗**
5. **Security Operations Engineer Jobs Indonesia ↗**
6. **Security Operations Engineer search Indonesia ↗**
7. **Security Operations Engineer job finder Indonesia ↗**

1. **Security Operations Engineer jobs↗**
2. **Security Operations Engineer jobs↗**
3. **Security Operations Engineer jobs↗**