CASE STUDY:

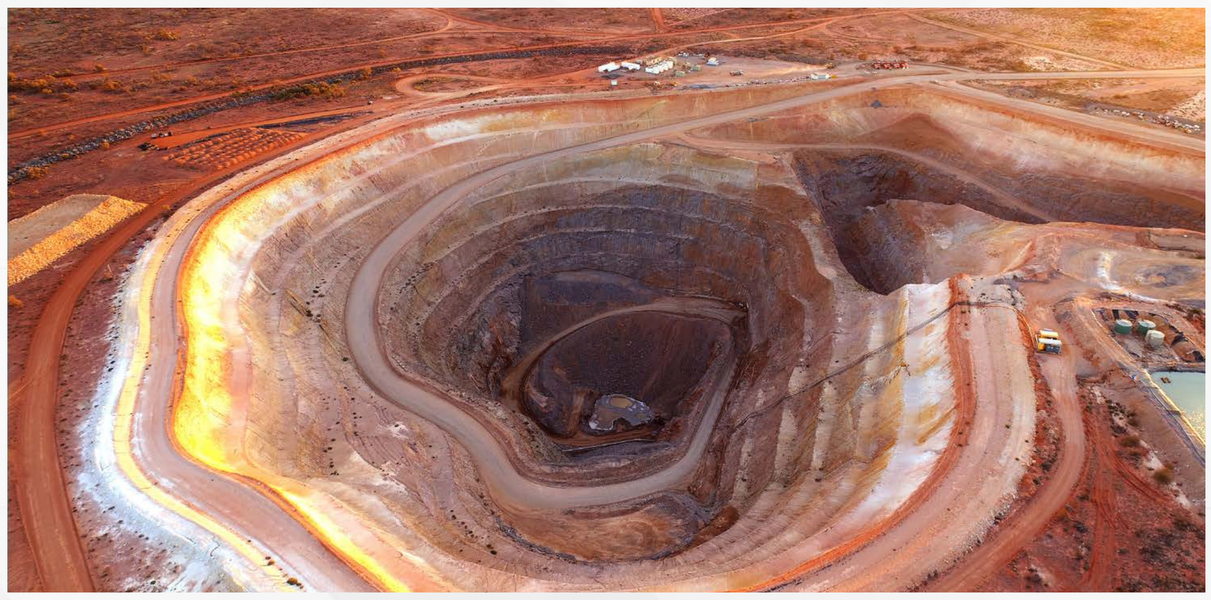
ALKANE
RESOURCES LTD

Red Piranha

Background

Alkane Resources is a gold production company with a multi-commodity exploration and development portfolio, presently producing between 50,000 – 60,000oz gold per annum. Listed on the ASX since 1969. Alkane presently has two core gold production assets, Tomingley & Peak Hill Gold Mine.

The Board and executive management at Alkane have always been security focussed. By engaging Red Piranha, Alkane has some of the best minds in Cyber Security at their disposal, providing guidance, support and assurance as Alkane works to improve their Cyber Security posture.



Industry Challenge

Mining companies are a major target of malicious actors. Performing a critical role in society, the consequences of a major technological disruption could seriously hinder manufacturing and export capabilities. Malicious actors are aware of this and target these companies, in hopes of eliciting a ransom. As an ASX listed company, Alkane is particularly exposed to Ransomware as a Service (RaaS).

The mining sector remains a valuable and vulnerable target for malicious cyber activity due to:

- highly sensitive personal data holdings
- valuable intellectual property related to underground /above ground mining, and ore processing plant operations
- the criticality of services delivered by the mining sector to the Australian economy
- pressure on mining sector organisations to maintain and, if disrupted, rapidly restore business continuity
- public trust in mining sector organisations.
- Perceived high level of affluence/available finances to afford/comply with large ransom amounts
- Dealing with large invoices which if fraudulently intercepted/redirected would be very profitable for the criminal

Understanding the extremely pervasive threat of cybercriminals targeting the mining sector, and the importance of a high level of cybersecurity maturity Alkane sought to protect their assets and gain a better understanding of any corporate cybersecurity vulnerabilities and to obtain a mitigation roadmap to address any vulnerabilities found. The Board engaged Red Piranha to conduct a Security Assessment and work with them to address any of the vulnerabilities raised.

Project Brief

Alkane engaged Red Piranha to provide Alkane Resources Ltd with

1. clear view of their security posture,
2. clear view of any lacking information security controls,
3. a security gap analysis,
4. recommendations, and a remediation roadmap
5. skilled resources to advise and assist with their information security policies and advise on enhancements to their information security technical controls

The abovementioned services were to be performed in accordance with industry best practise, pulling from various sources including ISO/IEC 27001framework and the Essential Eight strategies defined by The Australian Cyber Security Centre. Alkane's sites in Perth, Dubbo, Orange and Tomingley were in scope for this engagement.

Solution

Red Piranha Cybersecurity Assessment service

The Red Piranha Information Security Assessment allowed Alkane to review their pre-existing information security controls, identifying security gaps per industry guidelines, best practices, standards, and frameworks such as ISO 27001:2013, and the Australian Signals Directorate's Essential Eight and Strategies to Mitigate Cyber Security Incidents.

Red Piranha Limited's highly experienced personnel performed the Cybersecurity Assessment and provided remediation roadmaps for the adequate protection of Alkane's information assets.

Methodology

Red Piranha's Cybersecurity assessment services utilised a tailored gap-based approach to assess the internal controls and validated these controls against ISO/IEC 27001 and the Essential Eight.

The review was conducted by interviewing staff, examining existing security policies, processes, and registers.

Red Piranha utilised a three (3) phase approach for the ISO/IEC 27001 Gap Assessments as outlined below:

Phase 1: Understanding Organisation Structure

- ISMS & Risk Framework
- Information security team structure
- Obtain Information security policies & procedures

Phase 2: Gap Analysis

- Workshops
- Documented Review
- Gaps Identification

Phase 3: Reporting

- Executive Summary
- Gap Analysis Report
- Recommendations

vCISO- Virtual Chief Information Security Officer

Alkane Resources Ltd desired to increase and optimise their security posture and find solutions to reduce the scope of their exposure against a dynamic threat landscape with the goal of lessening the overall cost and burden of regulatory compliance. This included the requirement for a skilled resource to create and upgrade their information security policy structure.

Red Piranha's vCISO service provided the required outcomes through:

- Balance and management of information security risk factors.
- Assistance to the board and enterprise directors with meeting all current information security requirements.
- Comprehensive assessment of security posture to identify risks and optimise security posture over the short and long term.
- Approach to address dynamic threat landscape with industry standards, best practices, and regulations.
- High-level security service after a breach or security incident.
- Communication with stakeholders.
- Reporting to serve as a baseline, enabling Alkane to de-scope, re-architect and reduce exposure before proceeding.

Included in the vCISO service:

Information Security Policy Documents – 27000 Series

Red Piranha VCISO reviewed the current state of Information Security (InfoSec) and Cyber Security policies, processes and documentation and then provided Alkane Resources Ltd with documentation to increase InfoSec and Cyber Security standing.

One On-Site Board Meeting per year

Red Piranha's vCISO attended an annual meeting to update Alkane Resources Ltd's Board of Directors on the current and future state of Information Security (InfoSec) and Cyber Security and answer questions.

AGM ISMS Report

Red Piranha's vCISO created an annual report on Information Security Management System (ISMS) to be presented to Alkane Resources Ltd's AGM.

Remote ISMS Consulting

Red Piranha's vCISO provided remote support to Alkane Resources Ltd for an array of issues related to Information Security (InfoSec) and Cyber Security. This was conducted in a weekly meeting, and a monthly cadence meeting encompassing management stakeholders.

Quarterly Edge Vulnerability Scanning

A quarterly edge vulnerability scan was carried out by Red Piranha and scan results were shared with Alkane Resources Ltd along with recommendations to remediate any vulnerabilities. Red Piranha worked closely with Alkane's MSP to assist with the remediations.

GRC Risk Reporting

An annual report of security risks aligned to ISO 27000 series framework and status of compliance was prepared and delivered to Alkane Resources Ltd. As an additional service Red Piranha also prepared weekly Risk Reports for presentation to the Board.

Remote Incident Response and Escalation

Although no incidents occurred during the engagement, this service provided Alkane Resources Ltd with assurance and required ISO27001 compliance by having Red Piranha's 24/7/365 Security Operations Centre on call to address incidents within minutes.

Outcome

Red Piranha has provided ongoing support to Alkane via its vCISO program, assisting with policy and process development, implementation and industry compliance. As a result, the following security controls were implemented successfully

- Development of ISO/IEC 27001:2013 compliant polices to protect against internal and external threats.
- Cyber Security vulnerability scanning to continually audit company networks, systems, and applications for identified security vulnerabilities.
- Password Management and Multi-Factor Authentication programs to provide additional layers of user credential protection.
- Automated Anti-Phishing email filtering solution to mitigate the targeting of unsuspecting employees and protect access to company systems and data.
- Cyber Security Awareness Training to educate all staff in current cyber-attack techniques.

Alkane is committed to continually reviewing and improving their Security Posture. The Board has been proactive in continued development, with ongoing improvements planned in the following areas:

- Strengthening of access controls, IT, OT and IOT using network segmentation.
- Refining the company Cyber Business Continuity Plan
- Increasing infrastructure monitoring and Incident Response resilience.
- Active risk mitigation by correlating vulnerability identification, network activity and global threat intelligence.
- Ongoing Third-Party Supplier Risk assessment and compliance monitoring.

By engaging Red Piranha, Alkane has been able to drastically increase their Cyber Security posture. By implementing the controls listed above, Alkane has taken concrete steps in mitigating Cyber Risk and minimising the likelihood of being hacked or having a data breach. Their understanding and willingness to continually improve at a Board level means that Alkane is unlikely to be caught unawares by malicious actors and is actively taking steps to stop Cyber Security incidents before they even occur.

Red Piranha
unified threat management

www.redpiranha.net
info@redpiranha.net
+61 8 6365 0450 | +61 2 8089 1219

RedPiranhaSec
RedPiranhaSec
RedPiranha