QUANN RESCUE

QUANN INCIDENT RESPONSE

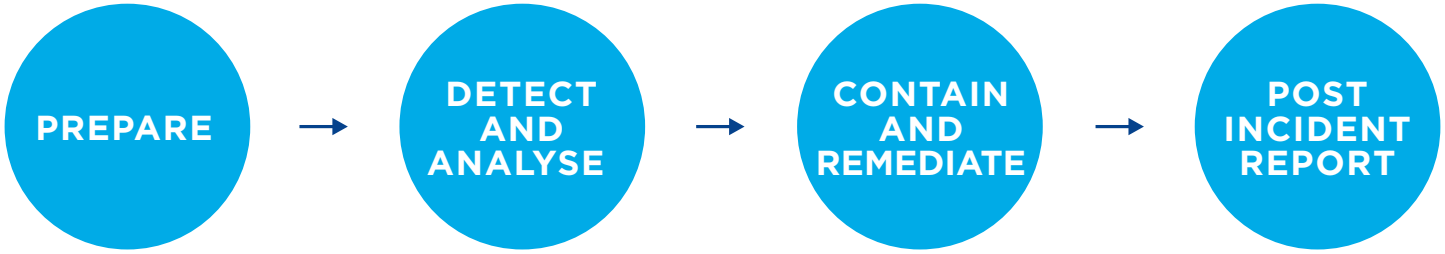
Get immediate access to security expertise for rapid response to cyber threats

IT security threats are becoming more and more sophisticated, and it is no longer a question of "if" but "when" an organisation will be attacked. If not well managed, these security incidents could have significant financial and legal implications and also cause long-lasting reputational damage. To minimise the impact of attacks, mitigate risk exposure and return to "business as usual" as quickly as possible, organisations need to be prepared and have a quick and effective response to cybersecurity incidents.

QUANN INCIDENT RESPONSE

Quann Incident Response helps organisations to manage security incidents to minimise any adverse impact on the business. It provides in-country support with 24x7 access to a team of experienced incident response security consultants who can provide immediate help to contain the breach, mitigate the threats and prevent further damage. They will also apply investigative techniques such as digital forensic imaging and analysis and malware reverse engineering to trace and eliminate the root cause of the security breach. Typical incident response and forensics engagements include, but not limited to, the following:

- **Network and application intrusion analysis**
- **Network, data and endpoint forensics**
- **Employee misconduct investigations**
- **Malware detection and reverse engineering**
- **Intellectual property theft investigations**
- **Electronic discovery and civil litigation support**



FEATURES

Dedicated hotline and email

- Organisations have 24x7 hotline and email access to Quann's security response team.

Response commitment

- Remote response will be provided within three hours of incident report.
- A specialist will be deployed on-site if further investigation is required.

Incident readiness assessment and recommendations

- We will assess your organisation's ability to respond to security incidents.
- Based on our findings, we will work with you to put in place response protocols and other recommendations to help boost your incident response capabilities.

Bundled incident response hours

- A pre-paid block of 20 man-days can be used for remote or onsite incident response support in the event of a data compromise.

Access to threat intelligence

- Statistics will be included in Quann Protect threat intelligence report.

BENEFITS

Immediate access to top-notch security expertise

Quann provides organisations with guaranteed access to well-trained and experienced incident response security consultants. Certified with technical and investigative skills, our consultants will provide immediate response to help organisations contain and remediate security threats.

Minimises business risk arising from cybersecurity

By providing swift response to cybersecurity incidents as well as email and data recovery, the Quann Incident Response helps organisations to mitigate risks, minimise the fallout from attacks, and resume normal operations quickly and efficiently.

Helps boost incident response readiness

Through the incident response assessment, organisations have better insights into your own ability to manage cybersecurity incidents. Recommendations and advice from Quann's incident response security consultants will then help you plug any gaps and fine-tune your incident response capabilities.

Prevents recurrence of security breaches with comprehensive forensics and investigation

Intrusion analysis, malware detection and reverse engineering, and comprehensive investigations into areas such as employee misconduct and intellectual property theft are some of the services that we do to help organisation trace the root cause of security incidents and prevent a recurrence.

QUANN
THE ART AND SCIENCE OF BEING CYBER SECURE

For more information, please contact us at **info@quannsecurity.com**
or visit our website at **quannsecurity.com**