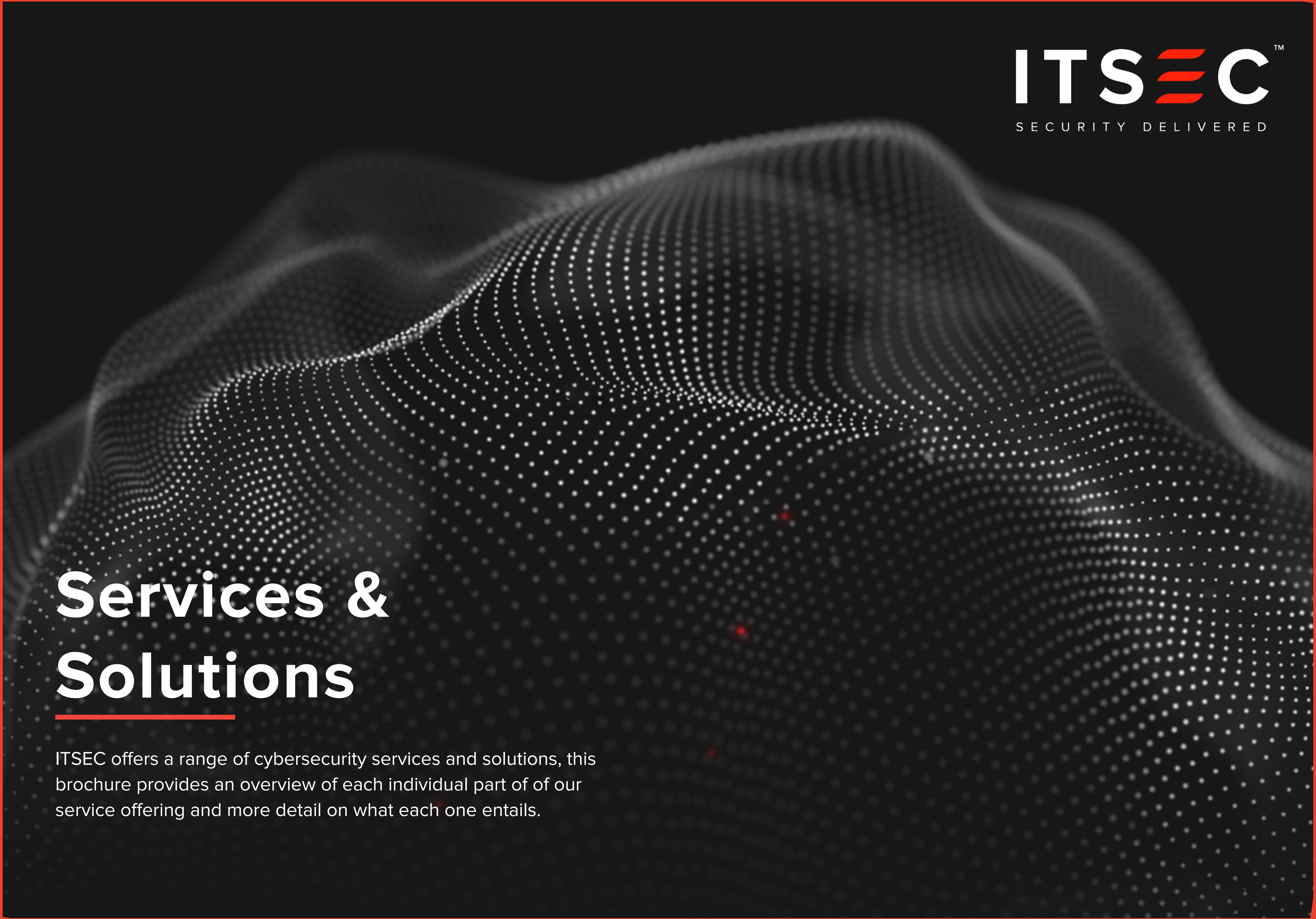


ITSEC™

SECURITY DELIVERED

Services & Solutions

ITSEC offers a range of cybersecurity services and solutions, this brochure provides an overview of each individual part of of our service offering and more detail on what each one entails.

Penetration Testing

Penetration testing assesses an organization's defenses by simulating an attack on their network. The process forms an important preventive measure. By identifying existing vulnerabilities and how an attacker would exploit them, organizations are empowered to proactively mitigate their security flaws. The process equips security teams with the knowledge and tools to circumvent an attacker's next move.

The quality of a penetration test lies in its ability to provide actionable insight. Rather than just outlining an organization's vulnerabilities and how they were exploited, ITSEC provides comprehensive post-simulation advisory services. A project report outlines all of the identified security vulnerabilities, along with a risk assessment and mitigation recommendations. ITSEC provides hands on training to ensure that mitigation steps can be implemented.

We also deliver presentations to various client stakeholders (ranging from executive management to security personnel), to ensure that an organization can respond at both a technical and strategic level

ITSEC has an industry-leading team that has delivered over 650 successful penetration testing projects. Our team has an extensive background in information security consulting services and cover a wide breadth of security domains including internal networks, web and mobile applications, as well as specialized areas such as RFID, ATM, EDC, and telecommunication infrastructure.

- **Breadth of Coverage**

  Stress test a range of security processes including data storage, access control policies, authentication mechanisms, and logging procedures.

- **Industry Best-practice**

  Implement the CREST approved method of penetration testing that combines black box (no knowledge of the target system), and white box (partial understanding of the system) approaches.

- **Dynamic Security Posture**

  Enables organizations to test their network against emerging threats and the latest tactics used by attackers.

- **Post-simulation Service**

  Remain actively engaged with a client after an attack simulation to ensure that mitigation steps are successfully implemented.

- **Well Documented**

  Final report includes details on identified vulnerabilities, risk assessments, and security recommendations.

- **Cohesive Approach**

  Combining technical, operational, and strategic mitigation steps.

Application Security

Software applications are now central to both an organization's internal operations and their interactions with customers. The security and integrity of an organization's applications is therefore now a strategic issue for the majority of businesses. This challenge has only intensified in recent years, with many large organizations now relying on several thousand software applications hosted on servers residing across the world.

ITSEC provides a variety of application security services that allow organizations to focus on the positive opportunities that arise from their applications. An extensive source code review process sits at the heart of our approach to application security. When combined with automated tools and manual penetration testing, our approach significantly increases the cost-effectiveness and security of our client's applications. Our team situate this process in a business context by understanding the specific purpose of an organization's applications and their coding practices, before delivering a severity risk estimate that accounts for both the likelihood of attack and the business impact of a breach.

We realize that applications are measured on more than just security. ITSEC therefore offers a variety of performance tests to compliment our security offering. We test the responsiveness and stability of applications under a high workload to ensure applications will remain reliable in a variety of business contexts. Our team of experts optimize applications against the highest standards in implementation, design and system architecture. ITSEC also provides various troubleshooting assistance and have the capability to analyse applications, databases, configurations, server logs, processes, etc.

- **Actionable Advice**

  We help our clients to implement processes to respond to any security or performance issues identified.

- **Security in Context**

  Application security assessments situate advice based on the specific challenges facing a client, with our risk assessments focused on practical business impacts.

- **Strategic Security Challenges**

  Our DevSecOps program introduces a culture of security to all the key personnel involved in strategy development, system design, transition, and operations in order to deliver a complete perspective on security.

- **Extensive Code Review**

  Our extensive code review is combined with automated tools and manual penetration testing to deliver significant cost savings.

- **Beyond Security**

  ITSEC's performance testing service strives to optimize the implementation, design, and architecture of a system.

- **Future-ready**

  Our insights into emerging technological trends mean our solutions are prepared for developments in technology and cyber threat landscape.

Information Security Analysis

The Information Security Analysis (ISA) service is one of ITSEC's key offerings and provides a comprehensive analysis of an organisations' cyber security posture. Our ISA service provides clients with industry-recognised best practices and is compliant with ISO27001/ISO27002 standards. The service has a wide ranging scope that includes a review of an organisations' information-system-security-policies, as well as the standard operating procedures around cyber-incident-management, business continuity, and disaster recovery. The process helps organizations to formulate and fine-tune their information security strategy. The service represents an excellent return on investment through optimised security measures and secure information infrastructure.

Our consultants cover both the technical and strategic aspects of information security management systems during the course of an ITSEC service delivery. Throughout an engagement, we focus on knowledge exchange with our clients to deliver a comprehensive training programme. A final project report contains assessment findings, any identified weaknesses, detailed remediation measures, as well as risk probability and impact assessments.

Our ISA service provides ensures robust business continuity in the event of an attack by developing a clear cyber incident response strategy. This equips organizations with the necessary processes and policies to effectively to both mitigate and respond to future cyber attacks. Our plans cover a variety of scenarios, ranging from unintentional data exposure, to data theft and full-blown network compromise.

- **Business Continuity**

  By having a business continuity plan in place, organisations give themselves the best chance of survival and are able to restore services quickly and smoothly.

- **Strategic Alignment**

  We ensure our cyber incident response strategies are aligned with an organization's broader business goals and priorities.

- **Beyond Prevention**

  Our SOC personnel have experience protecting a wide variety of digital infrastructure.

- **Industry Best-practice**

  Our advice is aligned with ISO27001/ISO27002 standards, providing our clients with an industry-approved cyber security strategy.

- **Wider Service Compatible**

  Our ISA service delivery complements wider services, such as penetration testing, to provide increased security awareness and a practical evaluation of implemented security measures.

- **Return on Investment**

  By optimising security measures, organizations reduce the likelihood of a costly attack.

Architecture & Process Development

ITSEC's Architecture and Process Development portfolio is a collection of methods that help organizations integrate security into their digital infrastructure. Modern businesses are increasingly embracing a variety of new technologies as they continue their digital transformation. This opens up a host of new opportunities, although also presents new risks. Digital transformation introduces further complexity into an organization's infrastructure that could be exploited by attackers.
ITSEC's portfolio of services ensures an organization's digital infrastructure is managed correctly and kept secure.

We help organisations to develop security policies that are aligned with their corporate strategy, IT strategy, and governance frameworks. However, a secure design requires more than just policy formulation We provide practical and hands on security design services.

These set out how to position the hardware and software used by businesses on a daily basis in order to achieve a high level of security.

As well as evaluating each component of a business's digital infrastructure individually, ITSEC also examines how different components interact to ensure there are no gaps in security across an organization's network that put critical assets at risk.

After a system is hardened and deployed, it is imperative that a high level of security. ITSEC ensures businesses have the processes in place to maintain security. This includes developing robust patching and update processes to ensure organizations retain a strong long-term security posture.

- **Managing Complexity**

  ITSEC's security design services evaluate how different components of an organization's digital infrastructure connect, ensuring any security gaps are fixed.

- **Security Maintained**

  Delivering a strong security posture is an ongoing process. ITSEC equips businesses with the processes to remain secure in the long-term.

- **Strategy Aligned**

  ITSEC works with clients to build security policies aligned them their corporate strategy and IT strategy.

- **Security Hardening and Baseline Establishment**

  Security hardening is the process of securing a system by reducing its attack surface and creating a baseline of system functionality and security.

- **Robust Policy**

  We design process models to enable organisations to produce integrated, operational and efficient information and cyber security policies.

- **Risk-based Approach**

  We provides a framework for organisations to ensure that their security objectives are reflective of risk tolerance.

We have a proven track record assisting clients with the following frameworks:

- ISO 27001
- Peraturan Otoritas Jasa Keuangan (POJK), the governing body of the Indonesian financial services sector.
- The European Union (EU) General Data Protection Regulation (GDPR)
- Threat and Vulnerability Risk Assessment (TVRA)
- Payment Card Industry Data Security Standard (PCI DSS)

Audits, Risk Assurance and Compliance

An information security audit provides an opportunity for businesses to take stock of their current approach. Audits cover a range of areas, including technical, physical, and administrative security measures. This presents an ideal foundation on which to build a coherent security strategy and provides a useful benchmark for delivering continuous improvements going forward.

Alongside our audit provision, ITSEC's Information Security Risk Assurance service helps organizations to be highly focused with their future security investments. We determine gaps in organisations' existing security policies, procedures, and controls before developing a plan to mitigate them as quickly as possible. Our team also evaluate current security investments to ensure they are delivering clear value. This process also allows us to ensure that an organization's cyber security investments link to their business objectives.

ITSEC also helps clients to navigate an increasingly complex regulatory environment. Our information security compliance portfolio provides a collection of services designed to ensure that our clients are following the latest regulatory frameworks.

We have expertise across a breadth of information security regulations, including both national and sector-specific frameworks.

- **Identifying Gaps**

  ITSEC's gap analysis helps to identify and remediate the holes in an organization's defenses.

- **Establishing a Foundation**

  Information security audits enable organizations to build a plan of their current security posture.

- **Navigate Complexity**

  Our team possess the expertise to guide clients through a range of information security regulatory and compliance frameworks.

- **Targeted investment**

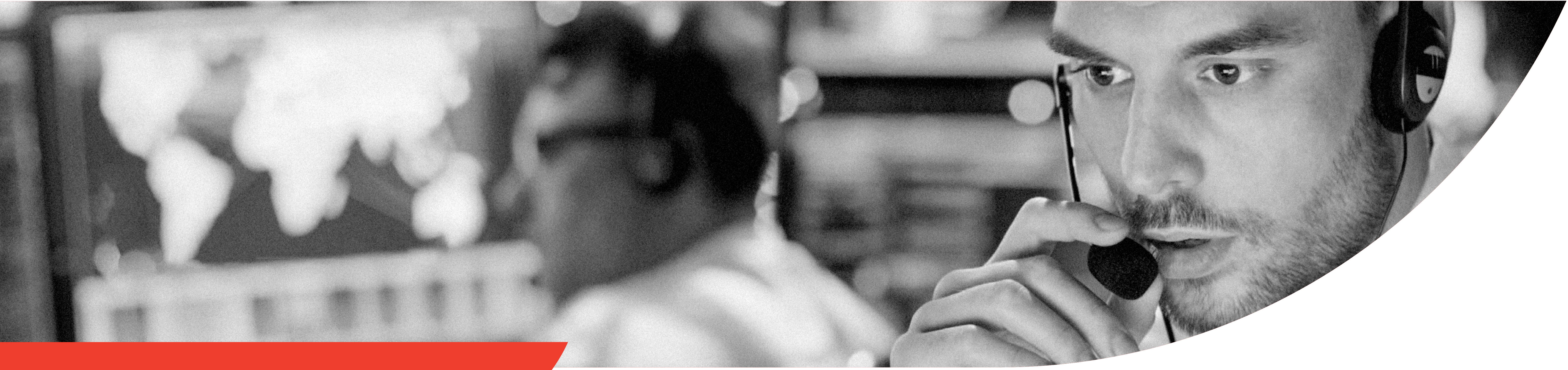
  Our assurance services ensure security investments are optimized to deliver maximum efficiency and value.

- **Mitigate Regulatory Risks**

  Organizations must ensure they have the processes in place to avoid what are increasingly costly fines that arise from non-compliance.

- **Executive Messaging**

  ITSEC helps security managers frame a business case for information security policies and investments, in order to gain buy-in from key stakeholders.



Managed Security Services

Protecting an organization from cyber attacks requires a long list of security processes that can quickly overwhelm even the largest organizations. Building the internal capability to deliver this also involves significant costs and resources. ITSEC's Managed Security Services (MSS) offers a solution to this problem, by providing a cost-effective outsourcing option where high quality security solutions can be delivered at pace. This equips organizations with an agile response to the latest threats.

Our MSS portfolio contains a variety of services that provide security at all stages of the defense lifecycle: prevention, detection and response. Our firewall monitoring service ensures that malicious traffic is blocked, while legitimate traffic is able to run smoothly through a network to ensure that good security does not compromise business processes. ITSEC also runs continuous vulnerability scanning on an organization's network to ensure flaws are fixed before they are discovered by attackers.

Through extensive network and log monitoring, ITSEC has the capability to detect and respond to attacks across a range of platforms including an organization's internal network, their cloud, and emerging technologies. Many of these processes require analysts to sift through thousands of alerts on a daily basis, many of which are false positive results. With ITSEC providing this service, businesses can instead focus on the positive opportunities that arise from embracing new technologies.

- **Agile Response**

  Our MSS portfolio allows organizations to shift their security burden to a managed service, allowing them to focus on positive business priorities.

- **Cost-effective**

  Our service is particularly beneficial for organisations that have resource constraints and a shortage of skilled information security professionals.

- **Access to Expertise**

  ITSEC experts act as an extension of your security team.

- **Continuous Monitoring**

  Our MSS portfolio....

- **Security at Scale**

  Our team of security specialists help organizations to quickly ramp up their security posture.

- **Defense-in-depth**

  ITSEC covers the whole defense lifecycle including prevention, detection and response.

Training

Cyber security is rarely static. The constantly changing nature of the cyber threat landscape means security teams must regularly update their skills and knowledge. This makes training an essential component in creating a dynamic approach to security. ITSEC takes a cohesive approach to security training that combines specialist programs for security teams alongside broader awareness-raising campaigns.

An organization's defense is only as strong as its weakest link. All employees must therefore play a role in mitigating security threats. Cyber security awareness training for non-security professionals is becoming an essential component of reducing risk. Employees from across an organization are getting tricked by sophisticated phishing or social engineering methods and too often provide an easy first entry point to sensitive information and data systems. ITSEC's cyber security awareness programs provide an extensive set of security awareness services to train corporate executives and secure their data.

ITSEC complements awareness training with specialist programs for security teams to build subject-matter expertise. For example, our Web Application Security program sets out how to integrate security throughout the entire software development lifecycle. The course offers a comprehensive action plan for each stage of a project. This ensures robust security is integrated throughout the development of software applications, rather than added as an afterthought. ITSEC provides also provides a range of other specialist courses, including telecommunication security training, X and Y.

- **Building a Culture of Security**

  ITSEC builds information security awareness across an entire organization.

- **Building a First Line of Defense**

  Any employee can be targeted through phishing and social engineering, meaning raising awareness can be one of the most significant changes an organization can make.

- **Secure Business Processes**

  Our Web Application Security program ensures security is integrated into existing business processes.

- **Secure Leadership**

  ITSEC fosters a security amongst executives, one of the most frequently targeted groups within an organization

- **Dynamic Security**

  Responding to the ever-changing threat landscape, requires security teams to constantly develop their knowledge.

- **Protect Business-critical Functions**

  We provide hands-on training to deal with telecommunication vulnerabilities to ensure business-functions remain secure.

Digital Forensic and Incident Response

ITSEC's Digital Forensic and Incident Response (DFIR) service works directly with organizations to investigate and respond to cyber attacks on their network. A DFIR capability is becoming an increasingly important component for organizations seeking to maintain business continuity in the digital era. Crucially, DFIR processes contain incidents as quickly as possible and prevent a cyber attack becoming a cyber crisis.

ITSEC's DFIR service combines technical and strategic advice to ensure all aspects of a cyber attack are managed effectively. Our approach combines a variety of processes, including identifying an initial attack vector, determining the extent of any compromise, understanding the attacker's methods and motivations, and developing an action plan to remediate. As well as implementing immediate steps to mitigate an attack, our team of consultants will also provide a report after the event to ensure appropriate steps are taken to mitigate future attacks. ITSEC also hosts tabletop exercises to enable organisations to prepare for potential future attacks.

Digital forensics is used to perform a systematic investigation while documenting the chain of evidence. Our method replicates the step-by-step actions of an attacker. We conduct an in-depth assessment of any suspicious activity and carry out an investigative analysis of computers, mobile devices, networks, memory drives, databases, logs, files, etc.

This allows organizations to fully grasp cyber incidents on their network and provides insight that can be fed into their long-term information security strategy.

- **A Complete Toolkit**

  ITSEC's DFIR service offers a portfolio of incident response processes to investigate and respond to cybersecurity incidents that hit organisations.

- **Attacks Contained at Source**

  ITSEC's DFIR service ensures that cyber attacks are quickly contained at source, minimizing business risk.

- **Systems Recovered**

  Our service aims to recover lost information, mitigating the impact of many cyber threats including ransomware and wipers.

- **Security Posture Prepared**

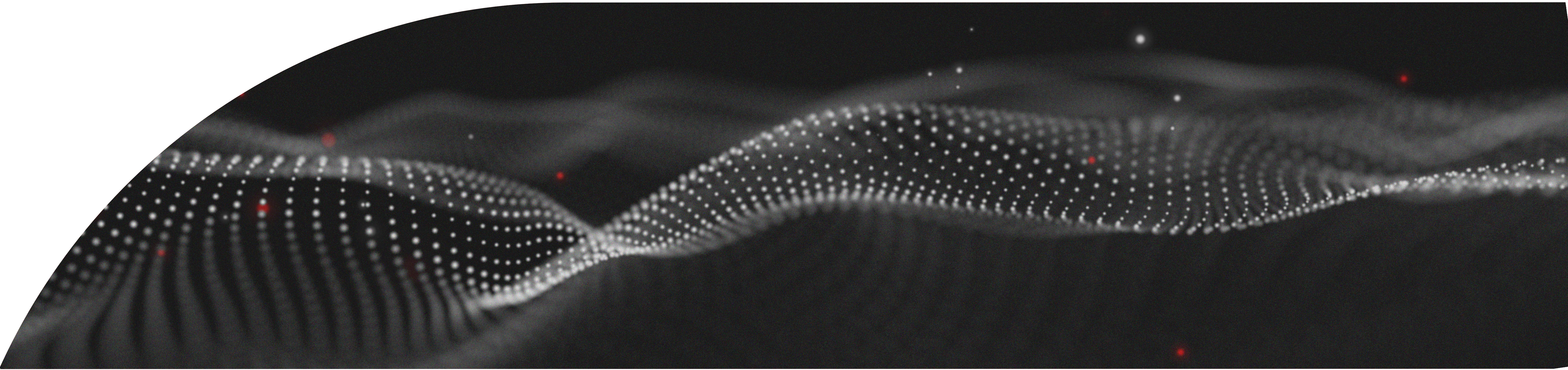
  ITSEC's Tabletop Exercise enables organisations to prepare for potential future security incidents and check their response processes are fine-tuned.

- **Strategic Insight**

  By understanding how attacks have bypassed a defense, organizations have the insight to address their flaws in their future information security strategy.

- **Broader Attack Context**

  We discover and analyse patterns of malicious activities to determine wider attack patterns.



Threat Hunting

Rather than waiting for an attacker to make their next move, threat hunting turns the tables around. By proactively probing networks, cyber threats that evade existing security measures can be detected and isolated. This disrupts even the most sophisticated threats who lurk in an organisation's networks and propagate across their infrastructure.

ITSEC has the tools, techniques and experience to identify and remove threats from an organisation's environment. We leverage threat intelligence and an extensive database of attackers' technical indicators alongside network sensors to trawl through an organization's infrastructure and ensure there is nowhere for attackers to hide.

We provide clients with a detailed report of our findings, which includes identification of any compromises (past or present) in their systems, accessed accounts, and any data obtained by attackers. Our security consultants uncover the complete threat context and determine any necessary remediation steps to respond to and eliminate threats. Our threat hunting services helps returns the advantage to the defender and gets an organization's security posture back on the front foot.

- **Proactive Security**

  Threat hunting puts attackers on the backfoot and returns the advantage to the defender.

- **Threat Context**

  Understand what is going on in your network and any associated risks that could emerge.

- **Forward-thinking**

  Our consultant provide detailed mitigation advice and threat reports for any attackers identified to prevent future attacks.

- **Inform Strategy**

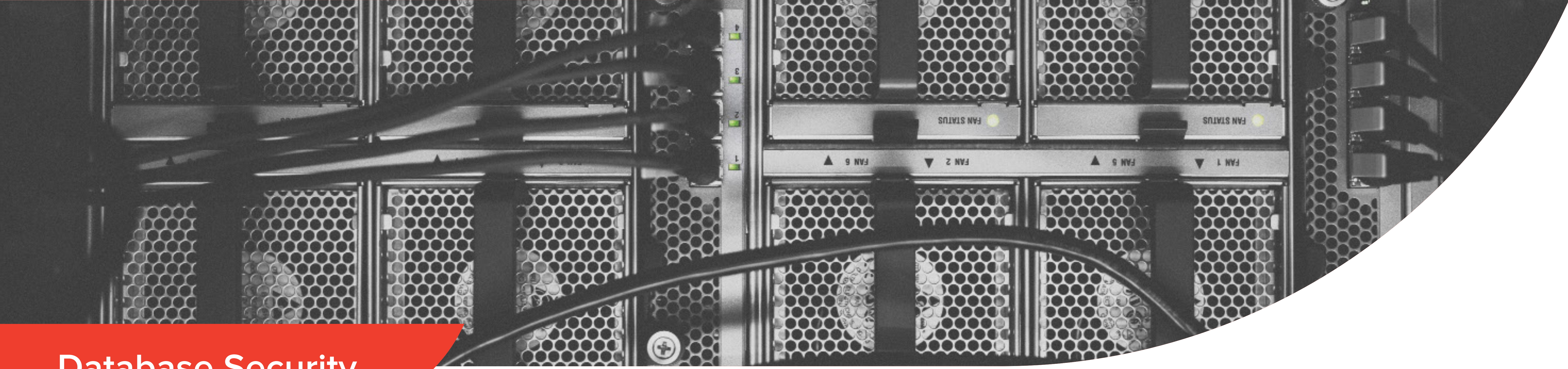
  Knowledge of the active threats on your network can be fed back into your cyber security strategy, closing the defensive feedback loop.

- **Intelligence-led Approach**

  We leverage threat intelligence and technical feeds from leading global cybersecurity firm.

- **Expert-led response**

  Benefit from ITSEC's expertise in responding to multiple attack groups, large and complex environments, extensive compromise, and complex remedial activities.



Database Security

Vulnerable databases expose organizations to a variety of risks and threats: ransomware attacks can cripple an organization's operations while the volume of information they hold make them the main source of data breaches. With databases often a single point-of-failure for organizations, their security should be at the core of every business's security strategy. ITSEC works with our clients to double down in ensuring both the integrity and security of their databases.

Understanding a database's vulnerabilities and exposure is an important first step in building robust security. Our database vulnerability assessment method includes sequential steps starting with preliminary interviews to analyse security requirements. It further consists of database artefact collection for detailed assessment, reporting essential assessment findings and discussing ways to strengthen security. Besides periodic security reviews, ITSEC works with our clients to assess database security during database upgrades and migration to new platforms.This allows businesses to remove the uncertainty and risk of implementing a bold digital transformation strategy.

Having established a database's vulnerabilities and exposure, ITSEC provides a database security hardening service. We ensure that all aspects of a database remain secure, including both software and hardware components, as well as client machines and firewalls.
Our experts then provide an assessment report that includes essential findings and recommended remediation actions. This allows organizations to radically reduce their attack surface.

- **Broad Expertise**

  We support a variety of databases including Oracle, Microsoft SQL Server, MySQL, PostgreSQL.

- **Reduce Attack Surface**

  With a multitude of attacks targeting an organization's database, ITSEC works with businesses to address some of their most severe threats.

- **Protect Business-critical Functions**

  Databases now sit at the core of almost all business operations making their security a core strategic issue.

- **Manage Digital Transformation**

  ITSEC helps organizations remove the uncertainty and risk of adopting new technologies and databases.

- **Defence-in-depth**

  ITSEC's database security assessment covers all aspects of a database, including hardware and software components as well as associated business processes.

- **Security Continuity**

  ITSEC ensures databases remain secure over the long-term.

Security Staffing

Recruiting and retaining security personnel represents some of the most significant security challenges facing businesses today. The pool of cybersecurity experts is small while the costs of dealing with cybercrime are mounting. This creates a difficult asymmetry for businesses who are struggling to confront the cyber security challenge with limited resources.

ITSEC works with organizations to bypass this problem. Many organizations are now turning to flexible, temporary and contract staffing models as a way to overcome the cyber security skills shortage. ITSEC embraces this model and partners with various companies to act as an extension of their security team. Relying on our talent network, we offer workforce solutions to organizations in a variety of regions and sectors. We guide businesses with our expertise in dispensing flexible staffing services, including temporary and permanent solutions.

Our clients benefit from our expertise, including access to our proprietary cyber security research and technical artefacts. Our consultants participate regularly in training and knowledge sharing sessions within our group, and pass on these insights directly to our clients.

- **Flexible Model**

  We guide businesses with our expertise in dispensing flexible staffing services, including both temporary and permanent solutions.

- **Cost-effective Security**

  ITSEC's talent network allows businesses to efficiently and quickly upskill their security team.

- **Instant Insight**

  ITSEC's proprietary cybersecurity research and technical artefacts provides vital information in preventing attacks.

- **Knowledge Sharing**

  Our consultants pass on the insight and expertise they gain through ITSEC's knowledge sharing program directly to clients.

- **Bypass the Skill Shortage**

  ITSEC provides businesses with access to talent without the associated recruitment and retention challenges.

- **Bespoke approach**

  Our solutions will be tailored to organisations' exact business requirements.

Security Operations Center

A Security Operations Centre (SOC) sit at the backbone of any security team. SOCs provide an essential function in monitoring and detecting any threatening event that is critical to an organisation's security. Organizations now host thousands of devices on their network, all of which are capable of providing data and alert. A SOC cuts through the noise and delivers security-critical situational awareness in the event of an attack.

ITSEC's state-of-the-art SOC is located in Jakarta, Indonesia and has been fully operational since July 2018. The SOC supports ITSEC's network of world-class security experts who act as an extension of your security team. Our SOC personnel are ready for when you need help the most and possess the resources to monitor, analyse, and defend your network. ITSEC's SOC actively protects a wide variety of digital infrastructure, including data centres, networks, servers, applications and databases.

ITSEC's SOC is based on our proprietary Information Security Process Manager (ISPM) that was developed in collaboration with security experts and software developers in Indonesia, Poland, and Singapore.

The ISPM's operational processes are automated, which result in increased productivity, reduced errors and cost savings that are passed directly onto our clients.

- **Crisis Ready**

  ITSEC's SOC will continuously monitor your network and is ready for when you need help the most.

- **Cutting-edge Technology**

  Our proprietary Information Security Process Manager utilizes advanced security technology to protect your systems.

- **Wide Coverage**

  Our SOC personnel have experience protecting a wide variety of digital infrastructure.

- **International Expertise**

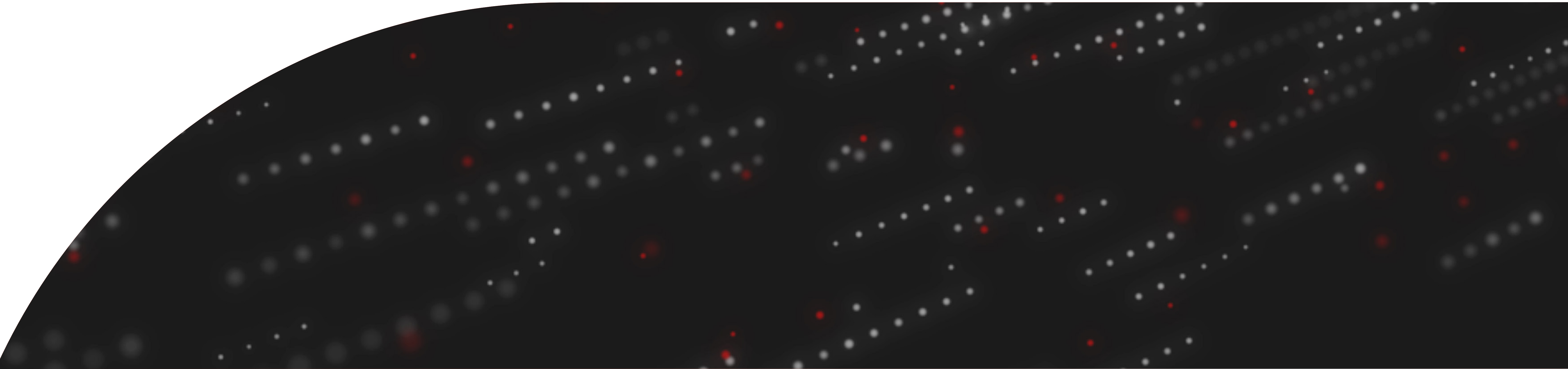
  Provide clients with access to world class consultants.

- **Proven Track Record**

  Since July 2018, ITSEC's SOC has mitigated countless attacks and vulnerabilities on behalf of its clients.

- **Remove False Positives**

  ITSEC's SOC converts heaps of data into digestible, actionable insight.



About ITSEC

ITSEC is one of the largest providers of information security services, solutions and technology in the Asia Pacific region, we employ 100+ employees and have more than 70 customers spread across our offices in five countries. You can find us at our headquarters in Singapore, or in our regional offices in Indonesia, Australia, Thailand, Saudi Arabia and the United Arab Emirates.

Singapore HQ

ITSEC Asia Pte. Ltd.
112 Robinson Road
#11-04 Singapore
068902

T: +65 9787 8322
E: info@itsec.sg
W: www.itsec.group

Indonesia

PT ITSEC Asia
RDTX Tower lt.28
Zona A Jl. Prof. Dr.
Satrio Kavling E.IV
No.6 Jakarta Selatan
12950, Indonesia

T: +62 (21) 57991383
E: info@itsec.asia
W: www.itsec.asia

Australia

ITSEC Australia Pty
Ltd. Level 19, 180
Lonsdale Street
Melbourne, Victoria,
3000

T: +61 1800 512 191
E: info@itsec.com.au
W: www.itsec.group

Thailand

ITSEC Thailand PTE
Ltd. Software Park
Thailand, Klongluer,
Pakkred,Nonthaburi,
Thailand 1120

T: +61 1800 512 191
E: info@itsec.group
W: www.itsec.group