Cybersecurity Consultancy Services

Risk less. Achieve more.

Contents

From advice to managed services, across the full security lifecycle

Be secure by design as you digitally transform

From identifying the risks in your environment to helping you manage it securely, we cover the full security lifecycle. We take you from roadmaps, architecture, solution comparisons and penetration testing to security-control implementations and managed security services.

Contact your Client Manager to discuss the security challenges you face and how we can help you address these.

Keep up with changing cybersecurity challenges

These include:

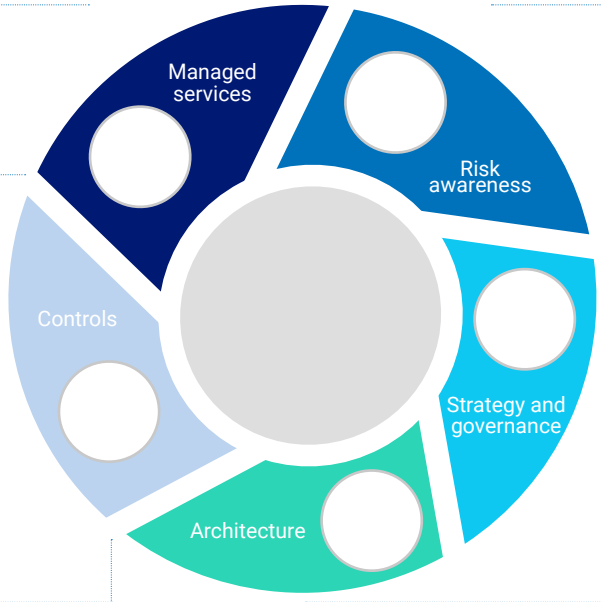
- **Increasing volume and sophistication of cyberattacks:** Absolute cybersecurity may be an impossible goal, but the right strategy and controls can mitigate your biggest risks.
- **Skills and expertise shortage:** There is a gap of 3.5 million cybersecurity professionals around the world, and the demand for security skills is only growing.
- **Increased governance, risk and compliance (GRC) demands:** GDPR, NISD, ISO 27001, CIS Controls, MITRE ATT&CK … business and IT activities must align to meet a growing list of global, regional and industry obligations.
- **The distributed business and a growing digital footprint:** COVID-19 has increased the digital footprint of organizations. They're now investing heavily in technology to support the new ways their employees, partners, suppliers and customers interact.
- **Cloud:** The move to cloud-based environments requires an adequate strategy for protecting cloud-based infrastructure.
- **Artificial intelligence and machine learning (AI/ML)** is helping businesses identify, detect and respond to threats faster than before – but it's also emerged as a powerful tool for cyberthreat actors.

Our top-down approach to security consultancy

We engage with you at all stages of the security lifecycle. We start by understanding your business and IT objectives and risks. From there, we develop security architectures that combine people, process and technology measures, in line with the Sherwood Applied Business Security Architecture (SABSA) framework.

Our client engagement model: the security lifecycle

- Security operating centers
- Cyberthreat intelligence
  - Vulnerability management
  - Managed endpoint detection and response (EDR) and extended detection and response (XDR)
  - Security orchestration, automation and response (SOAR)
- Security device management
- Digital forensics and incident response (DFIR)



- Unified threat management – firewall
- Web and email security
- Endpoint protection
- Cloud security
- Web application firewall
- Data and application security
- Identity and access management
- Intrusion prevention

Cybersecurity Consultancy Services

Our security profiles
- Governance consultants
- Architects
- Technology consultants
- Penetration testers

Our security competencies
- IT, Internet of Things, industrial control systems, operational technology
- Multicloud
- Identity and access
- Zero trust on identity, device, network
- Software-defined, LAN, WAN, data centers
- Data

To tackle the full security spectrum, our consultancy focuses on four key areas of managing cybersecurity risk, as per the National Institute of Standards and Technology (NIST) Cybersecurity Framework: identify, protect, detect, respond and recover.

We follow a variety of industry-standard frameworks (including NIST, ISO 27000 and IEC 62443).

Our security specialists cover the full security journey

From consultancy and security-control implementation to managed services, we have a broad range of security expertise and capabilities.

Our consultancy team includes:

- Security governance consultants (focusing on people and process)
- Security architects (focusing on business/IT needs and gaps to roadmaps and architectures)
- Security technology consultants (developing technical solutions)
- Penetration testers (covering the different security domains)

Our suite of Cybersecurity Consultancy Services

- **CISO as a Service:** Set up and operate Chief Information Security Officer (CISO) activities.
- **Security Advisory Assessment:** Evaluate your security maturity in terms of people, process and tools, according to GRC.
- **Secure IT Infrastructure Architecture and Design Service:** Ensure that your IT infrastructure is future-proof.
- **Secure OT/IT Consultancy:** Integrate cybersecurity into your smart factory initiatives.
- **Secure Multicloud Consultancy:** Accelerate your digital transformation by enabling a consistent, secure-by-design approach to your cloud journey.
- **Application Security Consultancy:** Incorporate security throughout the software development lifecycle.
- **Security Awareness Service:** Deliver customized security training to users and developers.
- **Penetration Testing Service and Red Team Service:** Test your systems, applications and infrastructure to identify exploitable vulnerabilities.

For more detail on the Security Awareness Service, Penetration Testing Service and Red Team Service, please ask your client manager for the specific NTT brochures

We engage with you at all stages of the security lifecycle. We start by understanding your business and IT objectives and risks. From there, we develop security architectures that combine people, process and technology measures.

CISO as a Service

The services of a knowledgeable cybersecurity adviser, backed by a team of experts

The changing face of cybersecurity and increasing need for reliable and secure information services have given rise to the executive role of Chief Information Security Officer (CISO) – but skills for these roles are both scarce and costly.

This can make it difficult to appoint a full-time internal CISO who is accountable for improving your cybersecurity posture in line with business priorities.

Ongoing advisory services through a holistic cybersecurity approach

CISO as a Service addresses this need by giving you access to one of our security advisers. They will collaborate with you to deliver a 360-degree view of the risks facing your organization. From there, they'll help you define and implement a cybersecurity strategy to address these risks.

They can also recommend appropriate security technologies and processes, and advise your management team on how to meet various security and privacy requirements for your industry and territories.

With CISO as a Service, you get access to an experienced NTT Security Adviser who can fulfill many of the requirements of an internally appointed CISO – either part time or as a dedicated resource to your organization

Because they can count on a wide pool of cybersecurity experts in our business, your Security Adviser will be well placed to answer your specific cybersecurity questions and address security requirements as they arise. They will help you to:

- Understand your risks, threats, current security measures and risk appetite
- Define your cybersecurity governance
- Define and maintain a tailored cybersecurity roadmap
- Follow the cybersecurity roadmap implementation
- Manage cybersecurity risks
- Define an awareness program
- Find solutions for day-to-day information security issues

Our approach and outcomes

Scoping and needs
- Define the scope of the Security Advisory Assessment
- Identify threat scenarios

2. Security Advisory Assessment
- Complete the assessment and issue a report
- Define the security roadmap, including defined project

3. Roadmap follow-up and reporting
- Follow up on execution of the roadmap
- Provide independent report on execution

4. Assistance with day-to-day security questions
- Give guidance on cybersecurity risk management
- Advise on security aspects of new projects

5. Increasing awareness in the organization
- Advise on how to run a security awareness campaign
- Follow up on the execution of the campaign

6. Benchmarking security in your industry
- Benchmark your organization's security against other enterprises in your industry, based on NTT's internal knowledge and external reports
- Give guidance on how to stay ahead of the security benchmark

7. Threat monitoring
- Regularly evaluate the relevance of your security roadmap in light of new threats

Security Advisory Assessment

A straightforward assessment to identify security gaps, and a strategic roadmap to close them

Security boundaries are constantly moving. Threats evolve rapidly and traditional networks can't protect your most valuable business assets. Business demands for mobile access, web-based applications and hybrid IT environments mean your IT landscape is changing just as fast.

With each new development, there's a new security risk. Regular reviews of the current state of your security architecture and processes are therefore critical to ensuring ongoing security and compliance.

Our Security Advisory Assessment not only identifies security gaps but also gives you a strategic roadmap to close them. This will help you to comply with external regulations and contractual mandates, align with industry best practices and ensure your security posture keeps pace with business needs.

Our Security Advisory Assessment identifies security gaps in the areas of people, processes and technology. We use this information to develop a strategic security roadmap, together with your stakeholders, that's aligned to your business and technology initiatives. This roadmap can be used to build a budget and resource plan to reduce the identified risks.

Choose your focus areas and level of detail

We customize our Security Advisory Assessment based on where you want to focus and the level of detail you need.

Our broad baseline assessment covers all areas of information security and includes people, process and technology domains. Alternatively, we can offer more focused assessments for multicloud, operational technology (OT) security, specific security controls (such as firewalls), security architectures and more.

Our approach and outcomes

We assess security risks from several angles, starting with clarity of vision and moving on to risk appetite, policies and assets all the way through to technical controls. From this assessment, we make specific recommendations on countermeasures.

Our methodology is based on standard frameworks like SABSA, ISO 27000, NIST and CIS.

We run a series of workshops with your stakeholders and conduct documentation and architecture reviews to:

- Identify internal and external security influences
- Define your current security state
- Determine risks and countermeasures.

We then project your current and target maturity states on to our Information Security Dashboard and Security Architecture Reference Model.

Maturity scale based on Carnegie Mellon (left side is current, right side is target)"

Maturity scale based on Carnegie Mellon (left side is current, right side is target)"

The result of our engagement is a strategic security roadmap for closing the identified gaps over the short and long term. We develop this roadmap with your stakeholders, taking into account your business priorities, risk scores and other considerations affecting security.

Secure IT Infrastructure Architecture and Design Service

Build architectures with embedded security to support your business

Changing your infrastructure architecture to support business needs is challenging enough. How do you ensure it's also resilient to the latest attack patterns in such a fast-evolving threat landscape?

This becomes increasingly difficult as your infrastructure becomes more open to the outside world and turns into a hybrid cloud architecture. The traditional perimeter-based and centralized security model has limitations in protecting your infrastructure and business production against risks such as lateral movement, malware propagation and credentials theft.

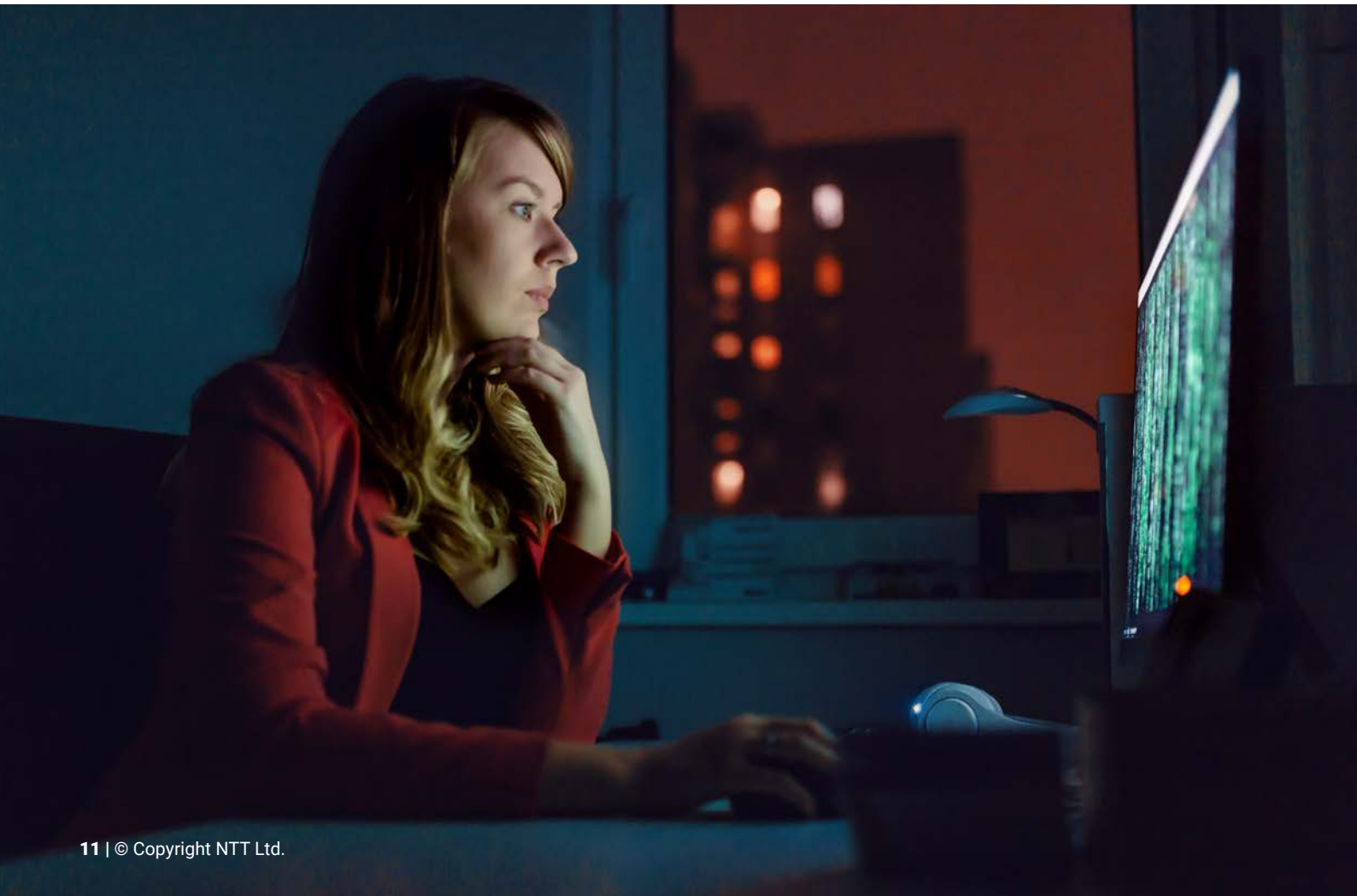
Even advanced architecture with granular network segregation may not be adequate for zero-trust architecture, private/public and hybrid cloud.

Our Secure IT Infrastructure Architecture and Design Service delivers expert recommendations for improving the resilience of your IT infrastructure architecture against attacks.

We have answers to your most pressing security questions

- How resilient is your infrastructure? Is the design of your architecture appropriate for protecting against security threats?
- What new, advanced hacking techniques can malicious users develop to put your production at risk?
- What new security controls, with proven efficiency, can you deploy in your infrastructure? And is it possible to do this without redefining your architecture form a greenfield?

We can give you reliable answers to these questions!



Your guide on the zero-trust journey

To identify and assess the risks inherent in your current infrastructure architecture, we perform a holistic review of your IT architecture. We then advise you on quick wins you can implement for short-term remediation as well as actionable recommendations for the medium term and long term.

Our proven consulting methodology is based on best practices from SABSA, CIS, NIST and other frameworks. We take a structured and comprehensive approach to each consulting engagement, following the six stages of our Consulting Services Lifecycle: engage, initiate, discover, analyze, recommend and conclude.

NTT's consulting services lifecycle

Manage								
Manage Expectations	Manage Scope	Manage Schedule	Manage Issues and risks	Manage Budget	Manage Internal team	Manage Status reporting	Manage Deliverable creation	Manage Follow-on opportunities

Engage	Initiate	Discover	Analyze	Recommend	Conclude
Prepare to engage	Assemble team and tools	Gather data	Analyze data	Develop recommendations	Confirm completion
Identify client need	Plan engagement delivery	Structure data	Define future state	Develop roadmap	Hand over opportunities
Qualify opportunity	Perform internal executive review	Define current state	Conduct gap analysis	Develop the case for change	Debrief stakeholders
Establish proposal team	Perform internal service review			Present deliverables	Close off services
Author, approve and advocate proposal	Conduct kickoff meeting/s				Review service delivery
Establish contract					

We take a top-down approach to review and build security architectures, starting with an understanding of your business goals, IT requirements and current overall architecture. This allows us to map to required security controls and technologies like zero trust, software-defined, virtualization and multicloud.

Our goal is a target security architecture – and a roadmap to get there – that's approved by all stakeholders.

We can also offer a security configuration assessment of key security controls, such as firewalls, web application firewalls (Wafs) proxies and remote access, as a separate engagement. Our review methodology is based on CIS Controls and CIS benchmarks as well as vendor best practices. This assessment gives you visibility of security gaps and risks, and concrete recommendations and a roadmap for closing them.

You'll receive a detailed and objective technical report that sets out our findings, the risks we've identified, evidence of key security controls and our recommendations.

Other deliverables include a risk register for cyber and technical risks, remediation plans, an investment plan for resource optimization and improved security, and target security architecture plan for your infrastructure to better protect your on-premises and cloud assets.

Secure OT/IT Consultancy

Lower the risk of major outages caused by security incidents and attacks

As operational technology (OT) and information technology (IT) have converged, industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems have become targets for hackers involved in terrorism, cyberwarfare, and espionage

Attacks on critical infrastructure such as power plants, factories, water treatment systems, oil rigs and traffic control systems can have far-reaching consequences, from reputational damage and financial losses to national security threats and even the loss of life.

Our Secure OT/IoT Consultancy can work with you to identify vulnerabilities in this area, develop a roadmap for remediation, and design a security architecture and network segmentation model for OT.

Helping you on your NIS compliance journey

We can assist you in taking the right steps to comply with the updated European Union (EU) Directive on the security of network and information systems (NIS2 Directive).

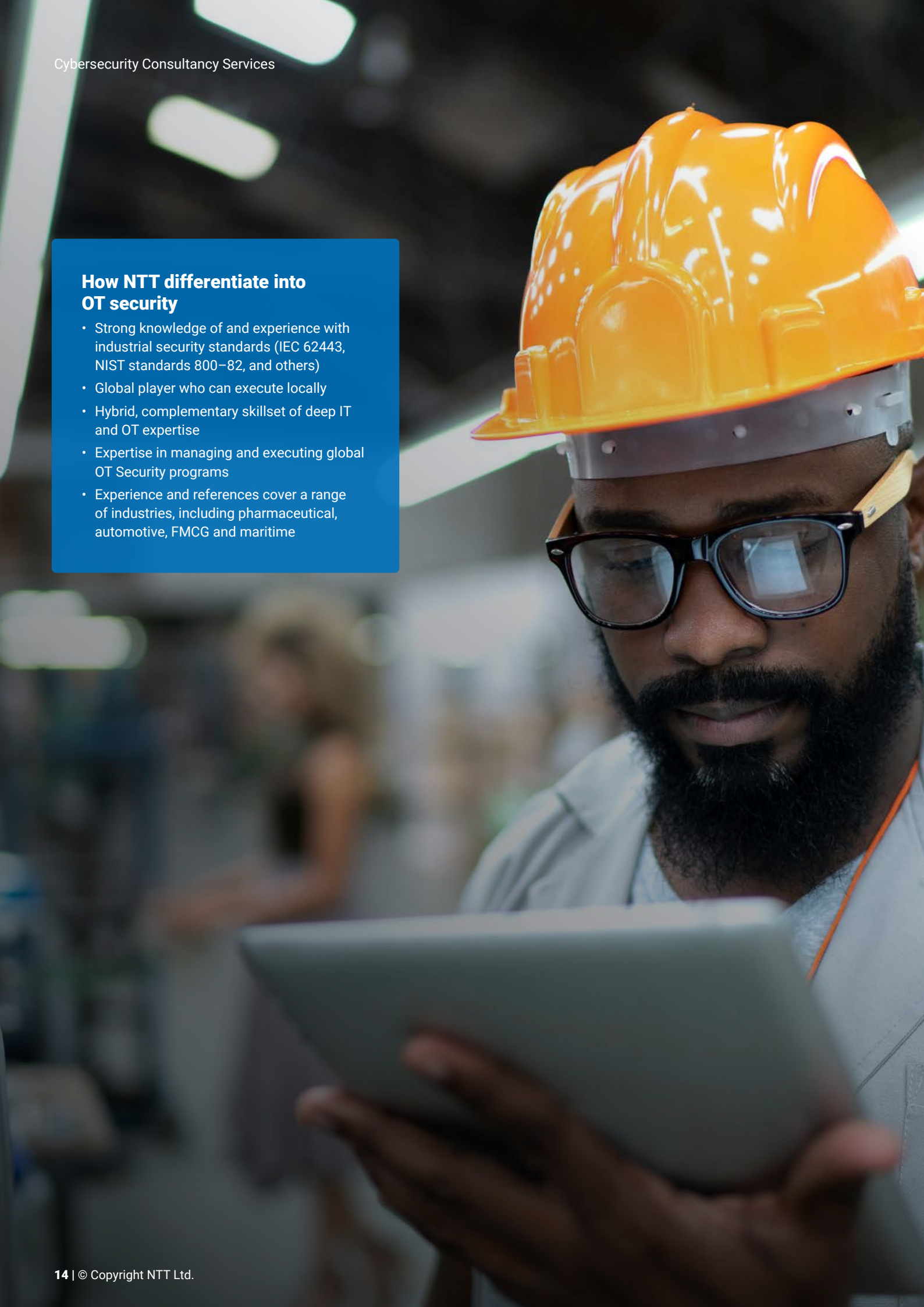
NIS2 not only requires higher levels of cybersecurity for compliance but also has a broader scope that addresses operators, the security of supply chains and supplier relationships. It also introduces the accountability of top management for noncompliance with the cybersecurity obligations.

From security assessments to managed services

We'll work with you to:

- Gain greater visibility of your OT assets, vulnerabilities, risks and security-control gaps through security assessments
- Develop a strategic security roadmap that covers people, processes and technology to close the gaps
- Design an OT security architecture and network segmentation model

NTT has built strong capabilities into the OT area. In addition to our consultancy services, we have a portfolio of OT products (including industrial switches, asset inventory, threat detection, vulnerability scanning, secure remote access and firewalls). We also offer OT installation, maintenance and managed services.



How NTT differentiate into OT security

- Strong knowledge of and experience with industrial security standards (IEC 62443, NIST standards 800–82, and others)
- Global player who can execute locally
- Hybrid, complementary skillset of deep IT and OT expertise
- Expertise in managing and executing global OT Security programs
- Experience and references cover a range of industries, including pharmaceutical, automotive, FMCG and maritime

Our approach and outcomes

Our end-to-end approach to OT security starts with knowing your assets, risks and current security controls. We then propose mitigations at the level of people, process and technology to increase security.

Securely bridging IT and OT

What you can expect from the Secure OT/IT Consultancy

Our **OT security assessment**, which can be tailored to suit your needs, includes the following steps:

1. Identify applicable framework/s

We identify the framework/s most relevant to your environment and industry sector (for example, industry standards such as IEC 62443 and ISO 27001 and the NIST regulations). We use this as our starting point for evaluating your security posture.

2. OT asset discovery

We deploy OT-specific tools to passively sniff and monitor your network in order to identify and validate your OT asset inventory. The inventory includes the device type, operating system, firmware version, device vulnerabilities and a security score of each device. This process builds a picture of how these assets are connected to each other and their respective placement levels within the Purdue (ISA-95) reference model.

3. Security assessment

We perform a comprehensive security risk assessment against the selected framework/s using a combination of document reviews, workshops, interviews and the technical results of the asset discovery.

4. Recommendations and reporting

We deliver a list of recommendations to close the identified security gaps. These recommendations are prioritized according to your operational risk profile and required timeframes.

Secure Multicloud Consultancy

Protection for applications, data and infrastructure across all your cloud environments

Cloud is an integral part of your organization's digital transformation – and cloud security is key to enabling new business initiatives while protecting critical data and assets.

Secure Multicloud Consultancy delivers a clearly defined and business-aligned cloud security program for securing your cloud environments**.**

We help you accelerate your digital transformation journey by enabling a consistent, secure-by-design approach to cloud across different delivery models (IaaS, PaaS and SaaS), in line with your strategic objectives.

Greater clarity for better security

We assess and advise you on your cloud security posture, architecture, and controls. This gives you clarity about what needs to be done, to what degree, and in what order.

Secure Multicloud Consultancy aims to:

- Give you a deeper understanding of your current risk profile
- Enable consistent cloud security controls, across multiple cloud platforms, by means of overarching security architecture and policies
- Simplify and optimize your hybrid security environment
- Offer uniform protection of cloud apps, data and infrastructure across all your cloud environments

Our approach and outcomes

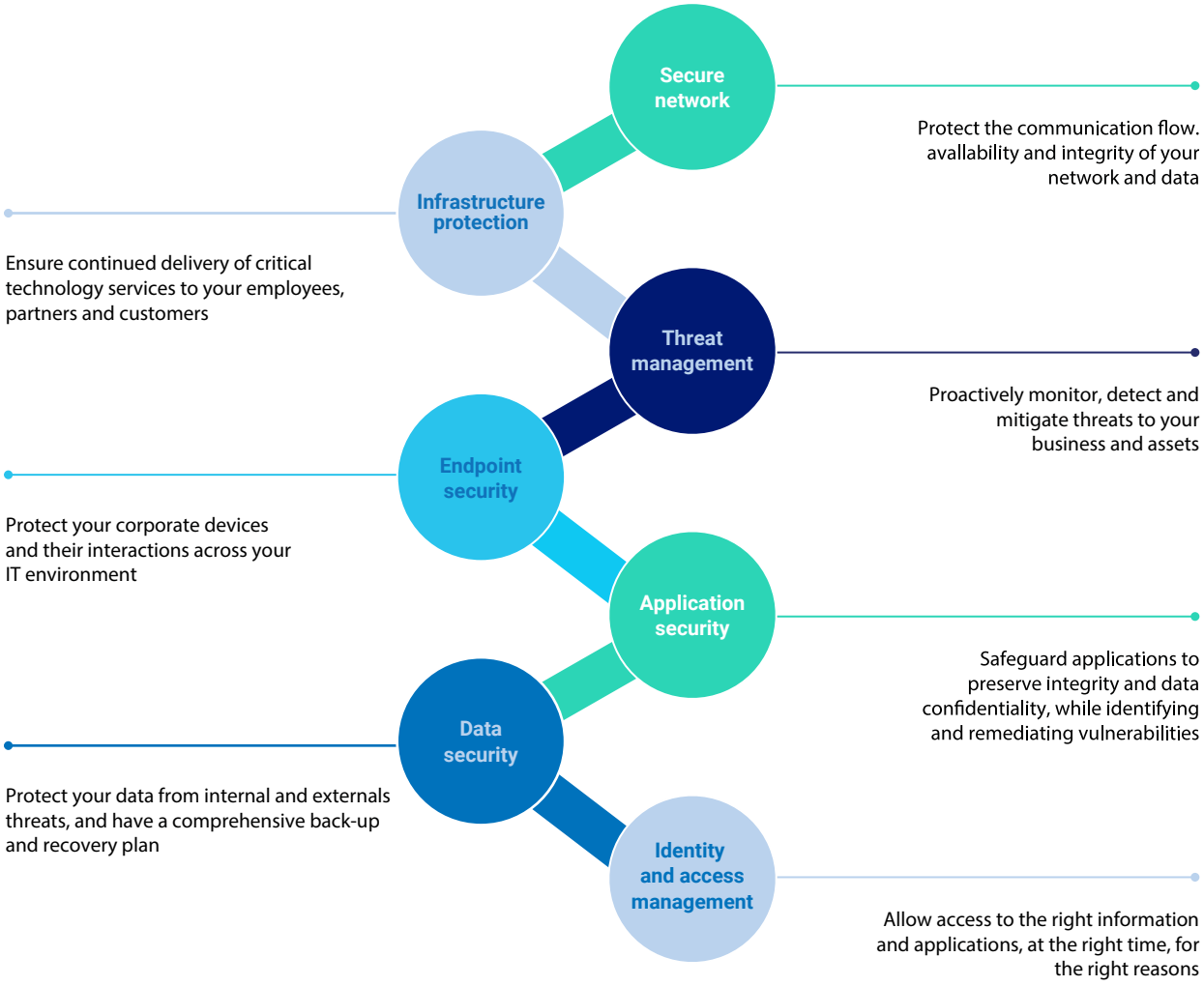
We help you understand the cybersecurity impact of moving to the cloud. We can also evaluate the maturity of your current cloud services and the effectiveness of your current controls.

We deliver our Secure Multicloud Consultancy service with the support of our cloud and security partners.

From an understanding of how all security controls operate in harmony to secure your organization, we then take a holistic approach to looking at the protection of cloud-based applications, infrastructure and data residing in your cloud environments. This gives you greater visibility of and insight into:

- Your security posture, risks, attack surface, assets and data flows and uniform visibility across the cloud landscape (IaaS, PaaS or SaaS)
- The appropriate mix of cloud-native or cloud-agnostic security controls
- How to enable your business with a holistic cloud strategy that minimizes risk and ensure compliance

We have the domain expertise you need
to secure your multicloud



By gaining visibility of your cloud resources across different environments, we can work out how best to secure your infrastructure using a combination of native and third-party controls. This includes:

- Ensuring effective and consistent governance, risk and compliance processes across your cloud environments
- How to manage the authentication and access to cloud resources through measures such as multifactor authentication and privileged access management
- Integrating security into your DevOps pipeline through ongoing vulnerability detection and remediation to prevent configuration mistakes
- How to automate security using policy guardrails, allowing continuous application of security requirements, leveraging cloud-scale benefits and agility.

The results are recommendations and an actionable roadmap for improving security processes and policies for multicloud estates, and a risk based and future-proof multicloud security architecture

Application Security Consultancy

Make API security work for you

Very often, the application programming interfaces (APIs) we find in most applications expose critical data such as personal identifiable information (PII). This makes them very attractive to attackers.

Our Application Security Consultancy can help you improve API security from development to implementation and operations.

Our engagements are immensely versatile and can be tailored to your organization's demand. We'll help you fine-tune your approach to application security to get to the level of maturity that's appropriate for your organization – taking both NTT technical and human aspects into consideration.

Smart security for API development

API security considerations should start at the early stages of application development and continue throughout the API lifecycle. We can help you define security strategies and control points to put in place to ensure proper governance and control over API development.

Security by design starts with properly trained developers

Implementing tools to perform **automated scans for vulnerabilities** within the development process is a good start. But if developers can't mitigate the risks of these discovered vulnerabilities, your security won't improve.

Our **Secure Coding Training** helps developers to understand the threat and vulnerability landscape so they can improve code maturity and reduce the risk of a vulnerability inside APIs (read on for more detail on our **Security Awareness Service)**.

A different perspective on application testing

We offer **application penetration testing** to test your applications from a different point of view. Instead of starting from the source code, our testers start from the hacker's perspective and actively look for weaknesses in the application (read on for more detail on our **Penetration Testing Service**).

Get more value from API security tools

API security tools can help you secure your APIs and detect any malicious activities. But it's not always that easy to understand, sort, and prioritize the vulnerabilities and incidents these tools reveal. **Our security consultants have the technical expertise to help you get more value from these tools – and the data that they generate.**

Our approach

Governance
- Strategy and metrics
- Policy and compliance
- Education and guidance

Design
- Threat assessment
- Security requirements
- Security architecture

Implementation
- Secure build
- Secure deployment
- Defect management

Verification
- Architecture assessment
- Security testing

Operations
- Incident management
- Environmental management
- Operational management

We can guide you on improving security at every stage, and on getting the most value out of the API security tools that are designed to support you during the implementation, verification and operations phases.

Our consultants work with your application teams to gain a deep understanding of your application environment. They then produce a comprehensive report that includes a proposed action plan or roadmap for resolving critical issues and improving the overall maturity of your API security.

Security Awareness Service

Training your first line of defense

Security awareness helps users and employees to understand the role they play in preventing and combating security breaches. It plays a vital role in your first line of defense against security threats.

Effective security awareness is more cost-effective than other solutions in preventing security breaches.

Employees who are security-aware understand that there are actors who will attempt to steal, damage or misuse the organization's data. Regular training helps them know how to respond to prevent this from happening.

We can help you build the most effective training schedule for your organization.

Our Security Awareness Service has four complementary modules

Our Security Awareness Service has four complementary modules

1. Secure code training for developers
2. (Spear) phishing simulations
3. The Cyberscape Game
4. A Security Awareness Program comprising more than 400 modules in 40 different languages

Ask your NTT Client Manager for a copy of our Cybersecurity Awareness brochure for more information.

Penetration Testing Service and Red Team Service

Penetration Testing Service

Controlled cyberattacks to discover critical vulnerabilities

New technologies bring potential risks to your IT infrastructure, giving attackers the possibility to disrupt and steal sensitive data.

Penetration testing services allow you to subject these new technologies to cyberattacks in a controlled fashion to make your IT infrastructure more resilient and determine if the technologies deployed are working as expected.

Our team

Acting as "ethical hackers", our team of consultants can test a variety of infrastructure, system and application technologies and frameworks, and a broad range of potential attack vectors.

Our team has a background in designing and implementing high-end IT infrastructures. They have more than 45 years' combined experience and a track record for discovering critical vulnerabilities in the most complex environments.

Our approach

We evaluate every layer of access in your operating environment, from outsider threats to the malicious insider.

This allows us to identify business-specific risks and determine how you can accurately target areas with the most risk, focusing attention where it's needed most.

Our engagements are immensely versatile and can be tailored to your organizations' needs. Our preferred method is to start with questions that challenge your current IT landscape:

- What's the real impact if an employee's machine is compromised while homeworking?
- Is your organization ready to withstand a sophisticated but realistic cyberattack?
- Are you able to identify active threats and shut them down?

Ask your NTT Client Manager for a copy of our Penetration Testing brochure for more information.

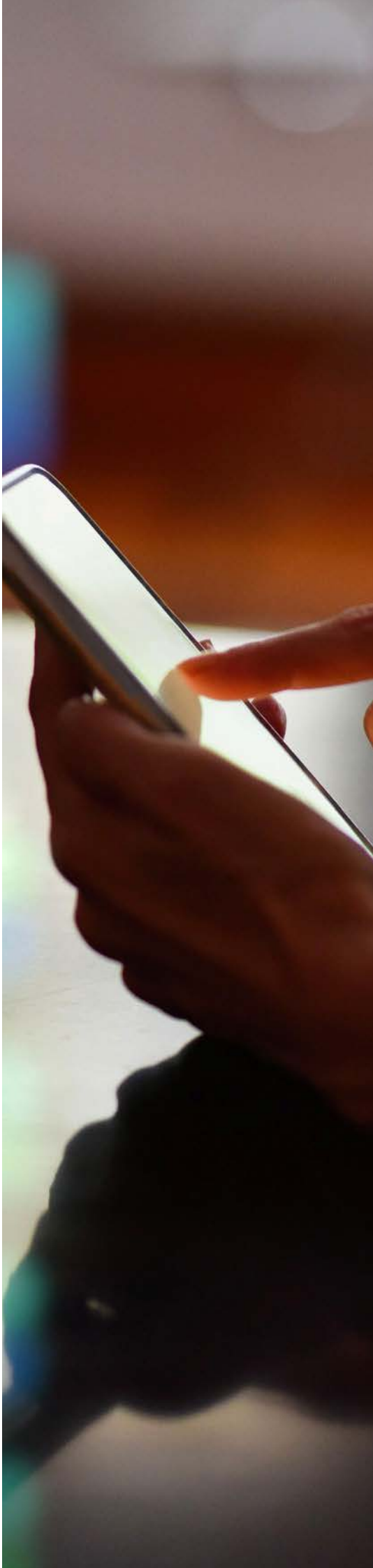
Red Team Service

Readiness through offense

Our Red Team simulates real-world attacks using similar tactics, techniques and procedures to those of known threat actors.

These exercises are performed in a controlled manner to train and improve your detection and mitigation strategies. They help you to uncover gaps in your security fabric which are not visible in normal day-to-day operations, and help you evaluate your current state of readiness for detecting and responding to breaches.

Ask your NTT Client Manager for a copy of our Red Team Operations Service brochure for more information.




NTT