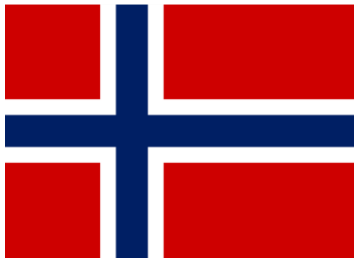
Atea One Security

Knowledge is Global
Business is Local

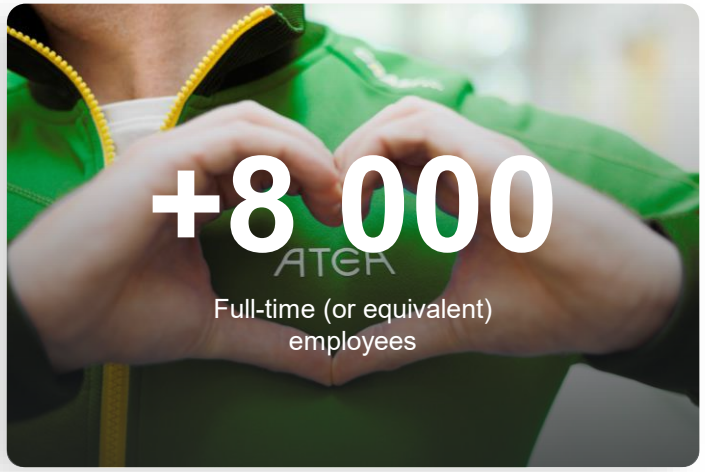




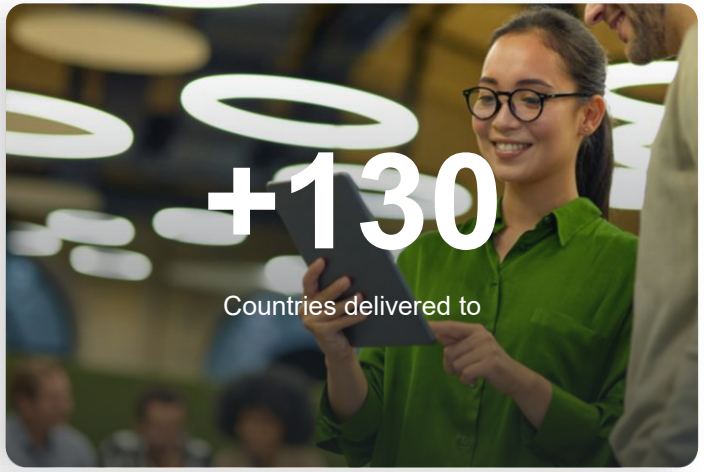




Audun Z Risberg – BDM Cyber Sec Atea Group
Vegard Kjerstad – Head of IRT Atea Group


+8 000
Full-time (or equivalent) employees


88
Offices


+130
Countries delivered to


3rd
Largest IT infrastructure company in Europe


1st
Market leader in IT infrastructure in the Nordic and Baltics regions


3,1
EUR billion revenue


ONE

The One Security Partner Portfolio

Our technology focus lies with our Strategic and Gold partners in Atea.

Locally Preferred Security Partners

ATEA

Atea Security Service Portfolio

Governance, Risk & Compliance (GRC)

Starting point: Sentry	Atea Custos toolbox	Security Awareness & Training	Risk Management	ISO, GDPR, NIS2, DORA, CIS ++	ISMS
		IT Law consulting	Policies & Procedures	Business Impact Analysis	vCISO

Security Technologies and Consultants Services

Post Quantum Technology	Network Security	Endpoint Security	AI Security	OT Security	Cloud Security
E-mail Security (anti phishing)	Application Security	Mobile Device Management (MDM)	Identity (IAM, PAM)	Backup/Recovery	SASE/SSE

Operational Security Services

Managed Backup aaS	MDR/XDR	SOC+	Incident Response Team (IRT)	Vulnerability Scanning	Penetration Testing

One Security Service Portfolio

Sentry – Custos (GRC)

The Sentry assessment is conducted as a three-day workshop, with aims of uncovering the “as is” and “desired” state of the organization's security posture. It is closely tied up with the NIS2 regulations, and concrete plans on how to improve compliance.

SOC+, MDR, XDR

Atea’s managed security services is tailored to meet both the public and private sectors in the Nordic and Baltic countries. With the three services, we meet the high demand from small, medium and large size organizations.

Incident Response (IRT)

This service emphasize on proactive elements, to make the organization prepared and more resilient. When an incident occurs, the global IRT is engaged. With experience from hundreds of incident, the team minimize the negative effect of a cyber attack

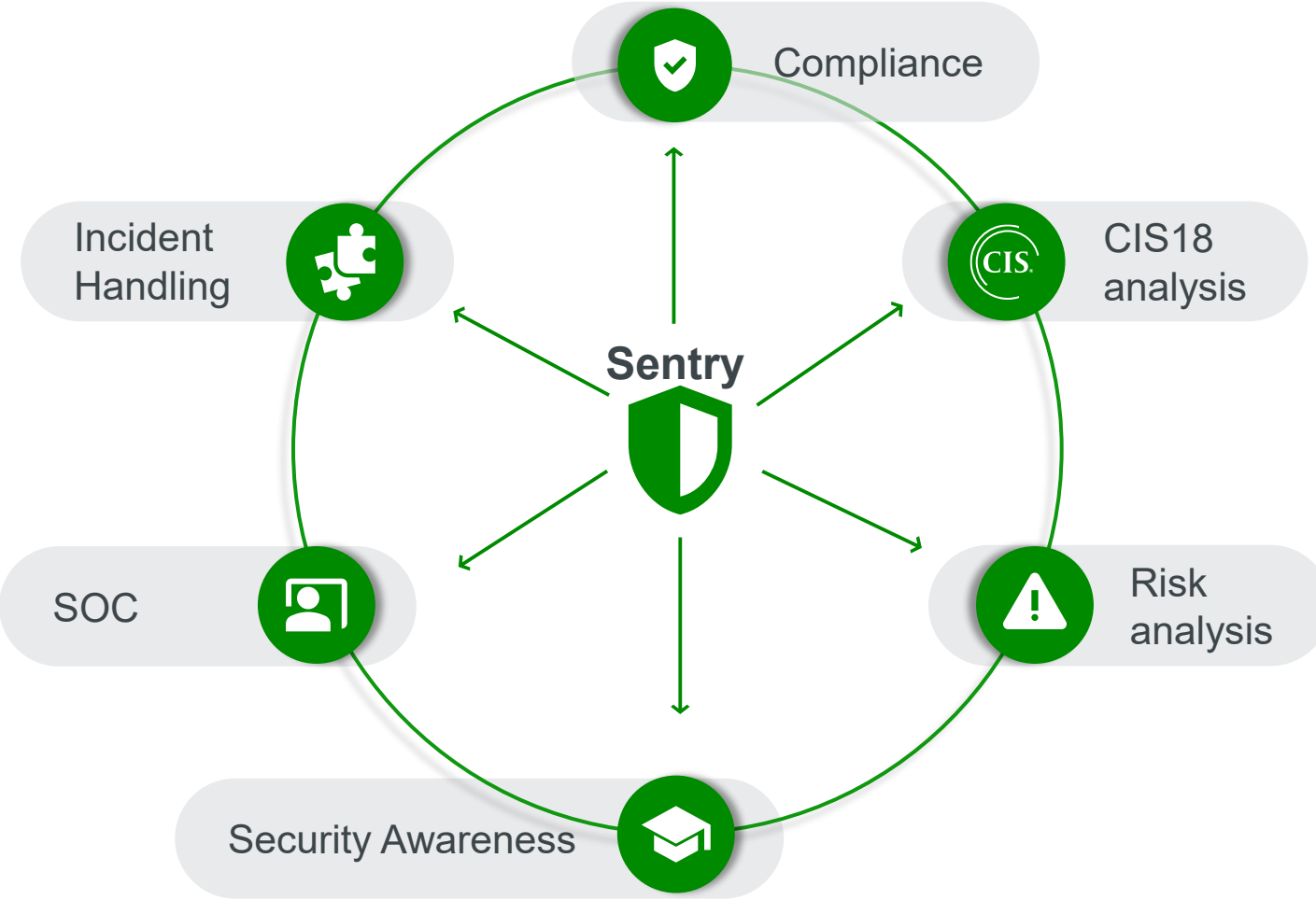
Atea Sentry

First step towards NIS2

Sentry is a three-day workshop that uncovers the “As is” state, and the desired state of the organization's security maturity and the level of compliance towards NIS2.

Sentry points out the suggested priorities and clarifies the journey ahed.

Built on Ateas Best Practice, NIST framework, ISO 27xxx and CIS



Atea Security Operations Services

- 24/7/365 monitoring and analysis of alarms – ensured by Atea SOC
- Optimized implementation and configuration
- Continuous configuration updates
- Proactive and automatic actions
- Automated IRT escalation

Premium

SOC+

24/7/365 monitoring ensured by Atea SOC

The premium offering includes all log sources, as well as support for firewalls, Kubernetes clusters, and other custom log sources as required by the customer.

Plus

MXDR

24/7/365 monitoring ensured by Atea SOC

The advanced offering that includes protection of end users, endpoints, email, cloud applications, all identities and servers. Protects against organization-wide threats.

Standard

MDR

24/7/365 monitoring ensured by Atea SOC

Protects end users and endpoints against threats. This tier includes the following product configuration, management and alarm handling:

Atea Incident Response Team

- Delivering one common IRT service to all Nordic and Baltic countries
- Utilizing Ateas global competence with local knowledge and customer closeness
- One IR operation, combining local and global resources
- Built on experience

The **reality** of a cyber attack

Financial loss

- Recovery costs
- Loss of revenue
- Ransom demand and payments
- Hiring external support

Operational issues

- Downtime for IT services
- Production halt
- Increasing backlog
- Communication halt

Compromised data

- Data theft
- Data deletion
- Data manipulation

Reputational damage

- Company “shamed” on attacker's website
- Loss of trust
- Loss of customers
- Negative media publicity

Regulatory issues

- Breach involving personal identifiable data (PII) poses GDPR concerns
- Fines
- Lawsuits
- Insurance claims

Physical and mental health

- Decision paralysis
- Loss of motivation and engagement from employees
- Extreme levels of stress and anxiety
- Increased sick absences
- Hospitalisation

Local

Presence

Represented with local presence and capabilities all over the Nordic and Baltic.

One IRT

Capabilities

- Lead incident handlers
- Incident responders
- Incident coordinators
- Forensics analysts
- Threat intelligence analysts
- Security researchers

Operational

During incidents

We can utilize the full width and scale of One Incident Response Team capabilities when needed

Our IR service has the best capacity and broadest skillset to offer

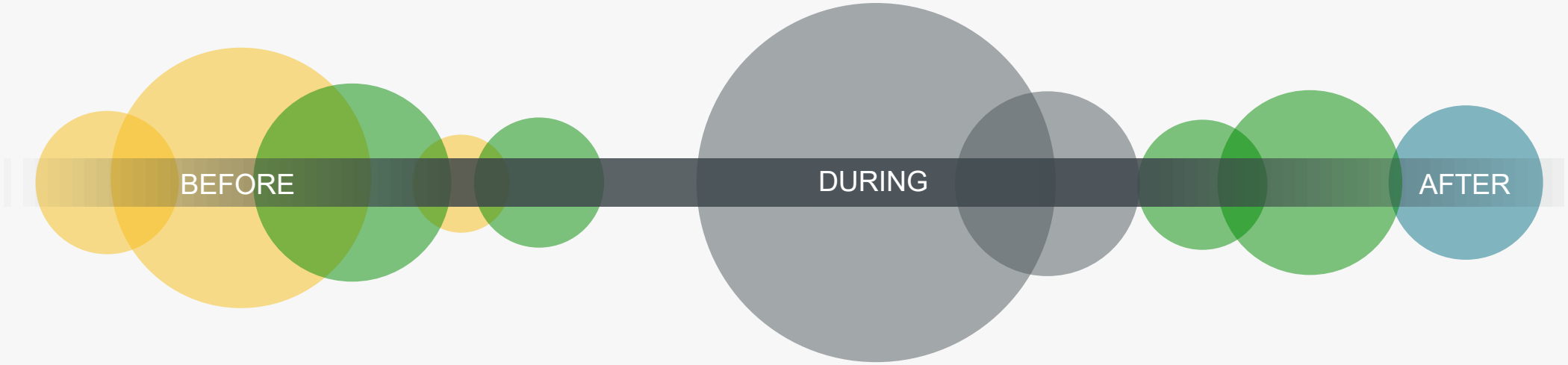
- GRC
- Network
- Endpoint
- Server
- Email
- Backup
- Cloud
- Security
- Identity
- Project managers
- OT
- Datacenter

With you every step of the way

Before, during and after an incident

Customer Security Advisor (CSA)
Regular meetings with a dedicated resource from IRT

After Action Review
Followed up by a fully documented report

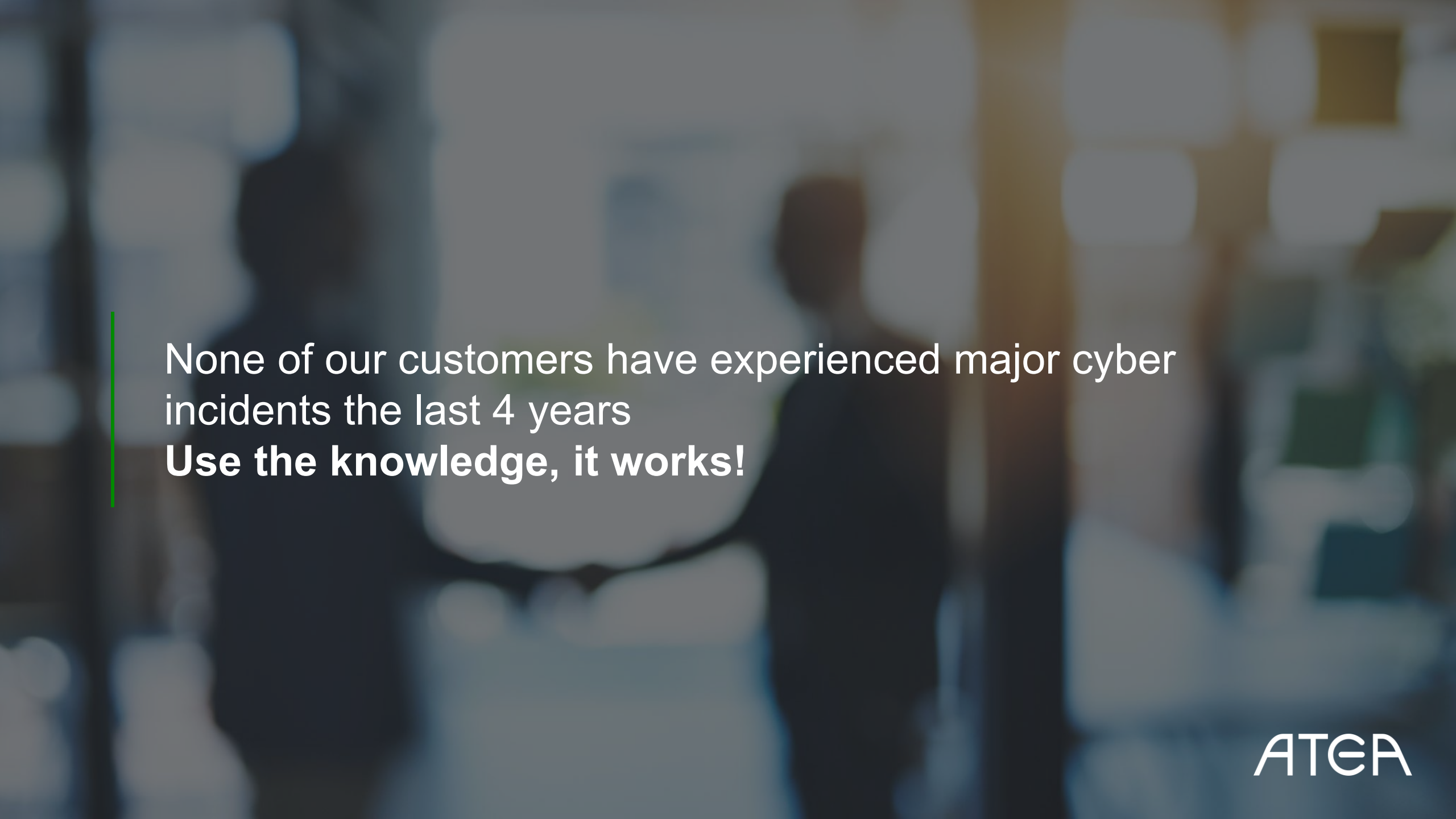


Comprehensive Onboarding
Strategic and technical Onboarding

Incident Response Team (IRT)
Purpose-built Incident Response Team

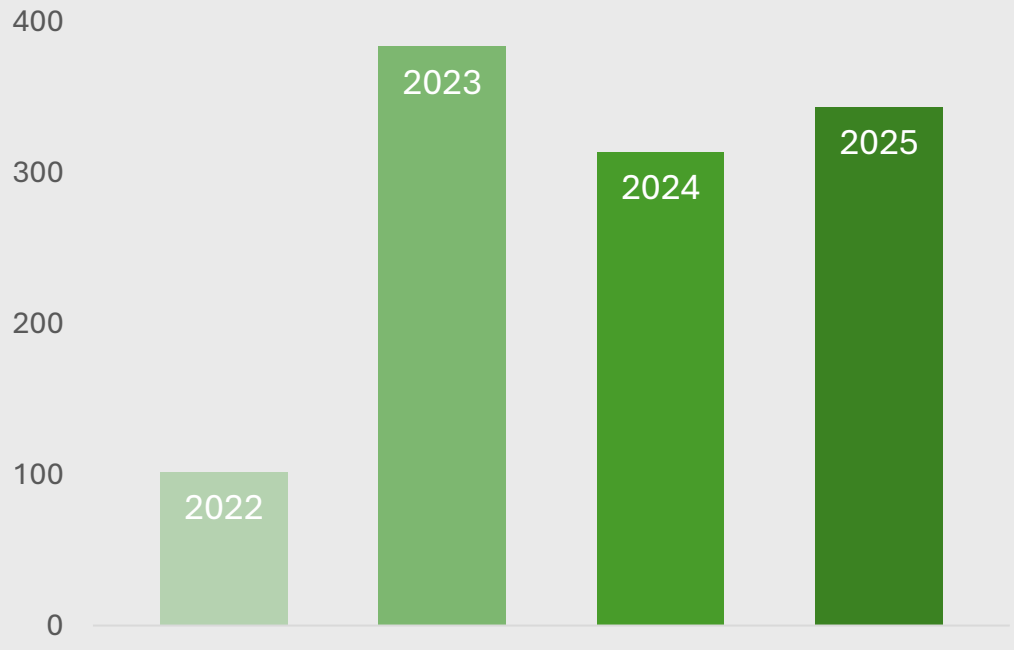
Proactive Capabilities
Advisory to limit the risk of being re-hit

Onboarding CSA IRT Proactive Capabilities


None of our customers have experienced major cyber incidents the last 4 years
Use the knowledge, it works!

Number of engagements per year

- No SLA breach for 4 years
- In 90 % of the engagements, we respond within 10 minutes



Cyber attacks we have been working on in 2026

- Ransomware
- APT hunting
- Adversary-in-the-middle (AiTM)
- Identity theft
- Financial fraud

…and what made them possible

- Vulnerabilities on Firewalls
- Lack of Multi-factor Authentication on Remote Access
- Lack of Phish resistant MFA for O365

The most common cyber attack

Adversery in the middle (AiTM) bypasses Multi Factor Authentication (MFA). You need phish resistant MFA.

Users' device

User presses a link and are redirected to a page where they are asked for sign in.

Attackers' device

Sign in is done from attackers' device instead of the users, without the user knowing it.

Cloud service

The cloud service only sees the sign in from the attacker's device, not the users.

ATEA

Five security recommendations

1. **Understand the threat landscape:**
   IT security is not only about technology, but also about people and processes. Stay up to date on current threats and how they may affect your organization.

2. **Strengthen basic security**
   Ensure that the organization has fundamental security measures in place, such as multi-factor authentication (MFA), regular updates, and data backups.

3. **Build a security culture**
   Most security breaches are caused by human error. Train employees regularly in security awareness and make sure they know how to handle suspicious inquiries.

4. **Have an incident response plan**
   When an attack happens, every second counts. Make sure the organization has a clear plan for how incidents should be handled, including notification, isolation, and recovery.

5. **Set requirements for suppliers**
   IT security does not stop at your own doorstep. Make sure that all suppliers and partners follow strict security requirements, so that your value chain does not become a vulnerability.

ATEA

Five security recommendations

1. **Understand the threat landscape:**
   IT security is not only about technology, but also about people and processes. Stay up to date on current threats and how they may affect your organization.

2. **Strengthen basic security**
   Ensure that the organization has fundamental security measures in place, such as multi-factor authentication (MFA), regular updates, and data backups.

3. **Build a security culture**
   Most security breaches are caused by human error. Train employees regularly in security awareness and make sure they know how to handle suspicious inquiries.

4. **Have an incident response plan**
   When an attack happens, every second counts. Make sure the organization has a clear plan for how incidents should be handled, including notification, isolation, and recovery.

5. **Set requirements for suppliers**
   IT security does not stop at your own doorstep. Make sure that all suppliers and partners follow strict security requirements, so that your value chain does not become a vulnerability.

ATEA

Five security recommendations

1

Understand the threat landscape:
IT security is not only about technology, but also about people and processes. Stay up to date on current threats and how they may affect your organization.

2

Strengthen basic security
Ensure that the organization has fundamental security measures in place, such as multi-factor authentication (MFA), regular updates, and data backups.

3

Build a security culture
Most security breaches are caused by human error. Train employees regularly in security awareness and make sure they know how to handle suspicious inquiries.

4

Have an incident response plan
When an attack happens, every second counts. Make sure the organization has a clear plan for how incidents should be handled, including notification, isolation, and recovery.

5

Set requirements for suppliers
IT security does not stop at your own doorstep. Make sure that all suppliers and partners follow strict security requirements, so that your value chain does not become a vulnerability.

ATEA

Five security recommendations

1

Understand the threat landscape:
IT security is not only about technology, but also about people and processes. Stay up to date on current threats and how they may affect your organization.

2

Strengthen basic security
Ensure that the organization has fundamental security measures in place, such as multi-factor authentication (MFA), regular updates, and data backups.

3

Build a security culture
Most security breaches are caused by human error. Train employees regularly in security awareness and make sure they know how to handle suspicious inquiries.

4

Have an incident response plan
When an attack happens, every second counts. Make sure the organization has a clear plan for how incidents should be handled, including notification, isolation, and recovery.

5

Set requirements for suppliers
IT security does not stop at your own doorstep. Make sure that all suppliers and partners follow strict security requirements, so that your value chain does not become a vulnerability.

ATEA

Five security recommendations

1

Understand the threat landscape:
IT security is not only about technology, but also about people and processes. Stay up to date on current threats and how they may affect your organization.

2

Strengthen basic security
Ensure that the organization has fundamental security measures in place, such as multi-factor authentication (MFA), regular updates, and data backups.

3

Build a security culture
Most security breaches are caused by human error. Train employees regularly in security awareness and make sure they know how to handle suspicious inquiries.

4

Have an incident response plan
When an attack happens, every second counts. Make sure the organization has a clear plan for how incidents should be handled, including notification, isolation, and recovery.

5

Set requirements for suppliers
IT security does not stop at your own doorstep. Make sure that all suppliers and partners follow strict security requirements, so that your value chain does not become a vulnerability.

ATEA

Five security recommendations

1. **Understand the threat landscape:**
   IT security is not only about technology, but also about people and processes. Stay up to date on current threats and how they may affect your organization.

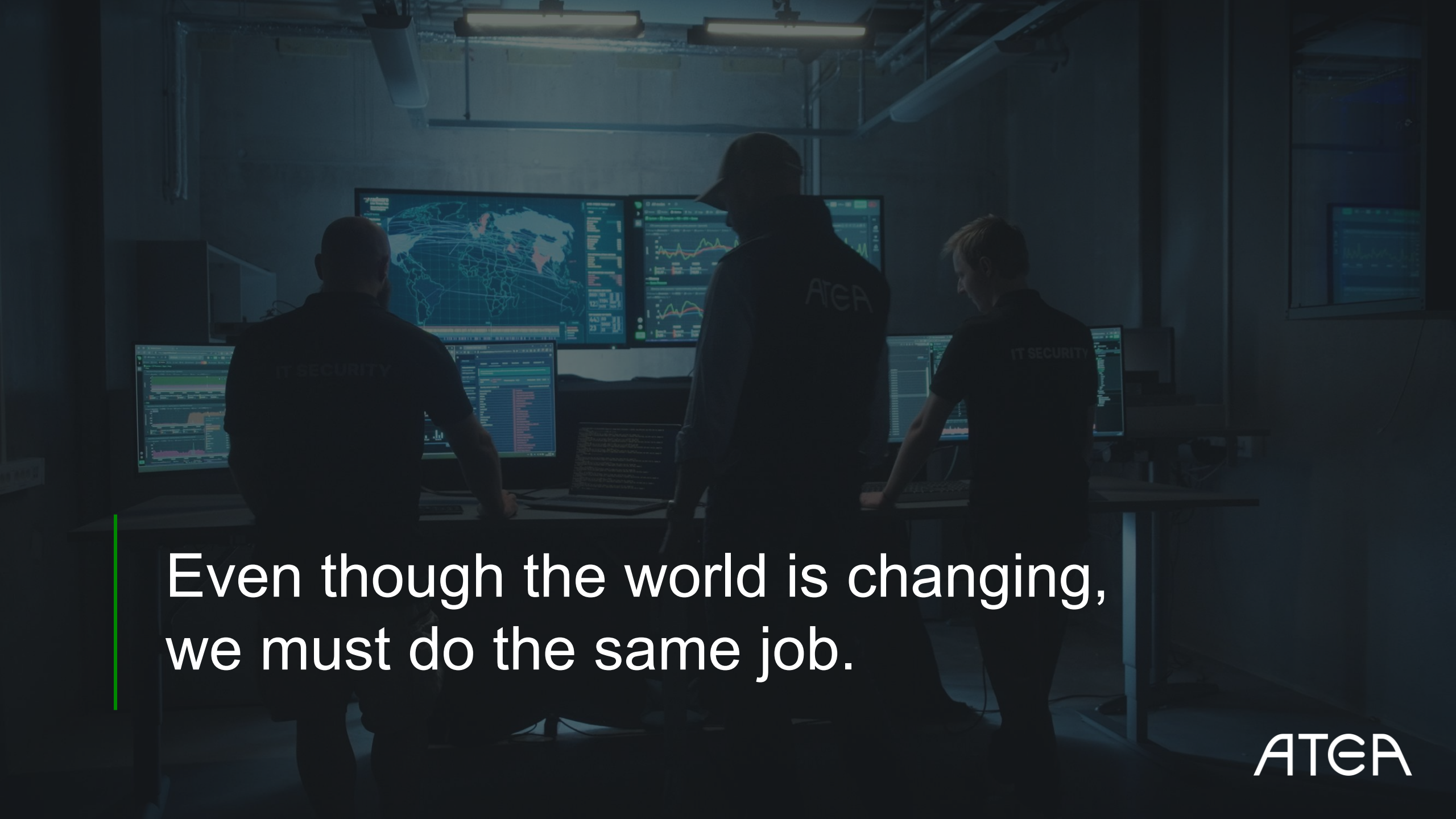
2. **Strengthen basic security**
   Ensure that the organization has fundamental security measures in place, such as multi-factor authentication (MFA), regular updates, and data backups.

3. **Build a security culture**
   Most security breaches are caused by human error. Train employees regularly in security awareness and make sure they know how to handle suspicious inquiries.

4. **Have an incident response plan**
   When an attack happens, every second counts. Make sure the organization has a clear plan for how incidents should be handled, including notification, isolation, and recovery.

5. **Set requirements for suppliers**
   IT security does not stop at your own doorstep. Make sure that all suppliers and partners follow strict security requirements, so that your value chain does not become a vulnerability.

ATEA

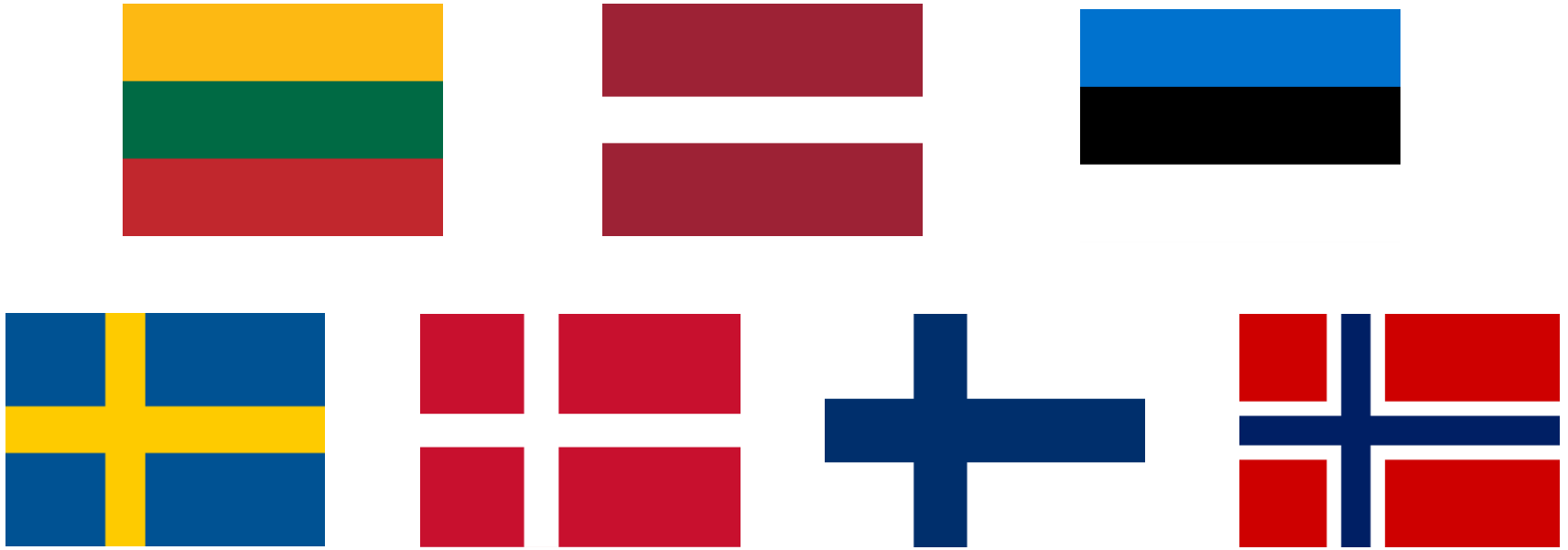


Even though the world is changing,
we must do the same job.

ATEA

Atea One Security

Knowledge is global, business is local



#TogetherWeSecureTheNordicsAndBaltics