CHECKLIST

DORA Compliance Checklist: Strengthening ICT Risk Management and Operational Resilience for Financial Services

How eSentire supports your organisation in managing ICT risks, enhancing resilience, and achieving compliance with the Digital Operational Resilience Act (DORA).

Introduction

The Digital Operational Resilience Act (DORA), formally known as Regulation (EU) 2022/2554, is a landmark regulation designed to harmonise and strengthen the management of information and communication technology (ICT) risks across the European Union (EU) financial sector.

As of January 2025, financial institutions and their critical third-party ICT providers will be required to comply with DORA's comprehensive risk management framework, ensuring they are prepared to protect, detect, contain, and recover from ICT-related disruptions.

These requirements are designed to reduce ICT risk across the EU's financial ecosystem, mitigate the impacts of cyber incidents, and ensure the continued operation of essential financial services, even during significant disruptions.

As such, DORA addresses two main challenges:

- **Comprehensive ICT Risk Management:** DORA introduces mandatory risk management frameworks for financial institutions and ICT service providers to ensure preparedness for all ICT-related incidents, including cybersecurity attacks, system failures, and natural disasters.
- **Harmonisation of Regulatory Standards:** Before DORA, ICT risk management regulations varied between EU member states. DORA establishes uniform standards across the EU, eliminating the complexity of navigating fragmented national regulations and ensuring a consistent approach to managing digital resilience across the financial sector.

DORA applies to traditional financial entities such as banks, investment firms, and insurance companies, as well as emerging sectors like crypto-asset service providers and crowdfunding platforms. It also extends its requirements to third-party ICT providers, such as cloud service providers and data centres, that deliver critical digital services to financial institutions.

DORA outlines specific technical requirements for financial entities and ICT service providers across four key domains:

- **ICT Risk Management:** Financial institutions must map critical ICT assets, perform gap analyses, and define risk tolerance levels to ensure the security and continuity of key business functions.
- **ICT Incident Management and Reporting:** DORA mandates detailed processes for classifying, managing, and reporting ICT-related incidents based on predefined thresholds.
- **Operational Resilience Testing:** Institutions are required to regularly test their ICT systems, security defences, and incident response mechanisms to identify and mitigate potential vulnerabilities.
- **Third-Party Risk Management:** DORA emphasises the need for continuous oversight of ICT-related third-party providers, ensuring that risks associated with outsourcing are closely monitored and tested.

Once fully implemented in 2025, DORA will be enforced by designated regulators in each EU member state, known as "competent authorities." These regulators have the authority to mandate specific security measures and impose penalties on non-compliant entities.

For critical ICT providers, the ESAs will appoint lead overseers with the power to levy fines up to 1% of a provider's daily worldwide turnover, ensuring that financial entities and their third-party providers remain aligned with DORA's standards.

With its focus on ICT risk management, incident reporting, operational resilience testing, and third-party risk oversight, DORA ensures that financial institutions are better equipped to withstand digital disruptions.

In this checklist, we break down the essential components of the DORA regulation and provide actionable guidance on how eSentire can help your organisation meet compliance requirements, enhance operational resilience, and manage ICT risks effectively.

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
ICT Risk Management	*Article 5: Governance & Organisation*	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organisation-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organisation's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. LEARN MORE **eSentire Virtual CISO (vCISO) - Security Policy Review and Guidance** eSentire's named Virtual CISO (vCISO) works directly with you to establish best practices for policies and procedures that align with key cybersecurity frameworks and compliance requirements. Under the guidance of our vCISO team, you will develop and implement your Information Security policies that address the highest priority areas of cyber risk. Our vCISO experts will conduct annual re-assessments of the policies to identify gaps based on applicable business, regulatory, or legal changes and support policy updates to address them. LEARN MORE **eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 6: ICT risk management framework	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 7: ICT systems, protocols and tools	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 8: Identification	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. LEARN MORE **eSentire Exposure Management** eSentire Exposure Management advisory services help you proactively identify gaps in your cybersecurity program, mitigate identified vulnerabilities, reduce your cyber risk, and build a cybersecurity strategy to improve how you anticipate, withstand, and recover from the most advanced cyberattacks. Our Exposure Management services are tailored to your business needs to help your organisation proactively identify gaps and refine your security strategy. LEARN MORE

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
ICT Risk Management	*Article 9: Protection and prevention*	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. LEARN MORE
	Article 10: Detection	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. LEARN MORE
	Article 11: Response and recovery	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. LEARN MORE **Digital Forensics and Incident Response** eSentire's On-Demand 24/7 Incident Response service guarantees you're prepared to withstand and recover from the most advanced attacks. Through a combination of best-in-class digital forensics technology and the expertise of our elite incident responders, we provide the fastest threat suppression in the industry so you can get back to normal operations in less than 4-hours. Our expertly trained incident responders provide full support through the investigative lifecycle, analyze the root cause of the attack, and help you address security gaps to prevent future attacks. LEARN MORE **eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE **eSentire Virtual CISO (vCISO) - Security Incident Response Planning** eSentire's named Virtual CISO (vCISO) works directly with you to develop a focused, pragmatic strategy that outlines key steps to take when a security incident occurs. Based on the initial assessment of your security posture, our vCISO team delivers a Cybersecurity Incident Response Plan. As part of the engagement, our team also conducts an annual reassessment of the plan and tabletop exercise to test the efficacy of the response measures. As your business objectives and environmental factors change, we work with you to update your Incident Response Plan to ensure it remains aligned with your goals. LEARN MORE

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
ICT Risk Management	*Article 12: Backup policies and procedures, restoration and recovery procedures and methods*	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 13: Learning and evolving	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE **eSentire Managed Phishing and Security Awareness Training** eSentire's Managed Phishing and Security Awareness Training puts you ahead of the latest social engineering cyberattacks and frees your internal resources from the time-consuming management of the end-to-end phishing program. We leverage software, social engineering expertise, and real-world testing scenarios to drive behavioural change with your employees. eSentire Managed Phishing and Security Awareness Training program extends beyond checking a compliance box, generating measurable results to ensure your organisation is resilient against the latest social engineering threats and business email compromise tactics. LEARN MORE
	Article 14: Communication	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 15: Further harmonisation of ICT risk management tools, methods, processes and policies	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 16: Simplified ICT risk management framework	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
ICT-related Incident Management, Classification, and Reporting	*Article 17: ICT-related incident management process*	**eSentire Virtual CISO (vCISO) - Security Incident Response Planning** eSentire's named Virtual CISO (vCISO) works directly with you to develop a focused, pragmatic strategy that outlines key steps to take when a security incident occurs. Based on the initial assessment of your security posture, our vCISO team delivers a Cybersecurity Incident Response Plan. As part of the engagement, our team also conducts an annual reassessment of the plan and tabletop exercise to test the efficacy of the response measures. As your business objectives and environmental factors change, we work with you to update your Incident Response Plan to ensure it remains aligned with your goals. LEARN MORE **eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE **Digital Forensics and Incident Response** eSentire's On-Demand 24/7 Incident Response service guarantees you're prepared to withstand and recover from the most advanced attacks. Through a combination of best-in-class digital forensics technology and the expertise of our elite incident responders, we provide the fastest threat suppression in the industry so you can get back to normal operations in less than 4-hours. Our expertly trained incident responders provide full support through the investigative lifecycle, analyze the root cause of the attack, and help you address security gaps to prevent future attacks. LEARN MORE
	Article 18: Classification of ICT-related incidents and cyber threats	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. LEARN MORE
	Article 19: Reporting of major ICT-related incidents and voluntary notification of significant cyber threats	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. LEARN MORE **eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
ICT-related Incident Management, Classification, and Reporting	*Article 20: Harmonisation of reporting content and templates*	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 21: Centralisation of reporting of major ICT-related incidents	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 22: Supervisory feedback	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 23: Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 24: General requirements for the performance of digital operational resilience testing	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE **eSentire Virtual CISO (vCISO) - Security Incident Response Planning** eSentire's named Virtual CISO (vCISO) works directly with you to develop a focused, pragmatic strategy that outlines key steps to take when a security incident occurs. Based on the initial assessment of your security posture, our vCISO team delivers a Cybersecurity Incident Response Plan. As part of the engagement, our team also conducts an annual reassessment of the plan and tabletop exercise to test the efficacy of the response measures. As your business objectives and environmental factors change, we work with you to update your Incident Response Plan to ensure it remains aligned with your goals. LEARN MORE **Digital Forensics and Incident Response** eSentire's On-Demand 24/7 Incident Response service guarantees you're prepared to withstand and recover from the most advanced attacks. Through a combination of best-in-class digital forensics technology and the expertise of our elite incident responders, we provide the fastest threat suppression in the industry so you can get back to normal operations in less than 4-hours. Our expertly trained incident responders provide full support through the investigative lifecycle, analyze the root cause of the attack, and help you address security gaps to prevent future attacks. LEARN MORE

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
Digital Operational Resilience Testing	*Article 24: General requirements for the performance of digital operational resilience testing*	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE **eSentire Virtual CISO (vCISO) - Security Incident Response Planning** eSentire's named Virtual CISO (vCISO) works directly with you to develop a focused, pragmatic strategy that outlines key steps to take when a security incident occurs. Based on the initial assessment of your security posture, our vCISO team delivers a Cybersecurity Incident Response Plan. As part of the engagement, our team also conducts an annual reassessment of the plan and tabletop exercise to test the efficacy of the response measures. As your business objectives and environmental factors change, we work with you to update your Incident Response Plan to ensure it remains aligned with your goals. LEARN MORE **eSentire Exposure Management** eSentire Exposure Management advisory services help you proactively identify gaps in your cybersecurity program, mitigate identified vulnerabilities, reduce your cyber risk, and build a cybersecurity strategy to improve how you anticipate, withstand, and recover from the most advanced cyberattacks. Our Exposure Management services are tailored to your business needs to help your organisation proactively identify gaps and refine your security strategy. LEARN MORE **eSentire Penetration Test** eSentire's Penetration Testing helps you understand how effective your privacy and security controls are, before a malicious actor breaks into your environment, causing business disruption. Our penetration testers use the latest tactics, techniques and procedures (TTPs) in an authorised attempt to gain access to your resources without the knowledge of usernames, passwords, and other usual means of access. In the post-penetration testing report, we provide a detailed summary of high-risk systems and recommendations on how you can improve your security posture. LEARN MORE **Digital Forensics and Incident Response** eSentire's On-Demand 24/7 Incident Response service guarantees you're prepared to withstand and recover from the most advanced attacks. Through a combination of best-in-class digital forensics technology and the expertise of our elite incident responders, we provide the fastest threat suppression in the industry so you can get back to normal operations in less than 4-hours. Our expertly trained incident responders provide full support through the investigative lifecycle, analyze the root cause of the attack, and help you address security gaps to prevent future attacks. LEARN MORE
	Article 25: Testing of ICT tools and systems	**eSentire Exposure Management** eSentire Exposure Management advisory services help you proactively identify gaps in your cybersecurity program, mitigate identified vulnerabilities, reduce your cyber risk, and build a cybersecurity strategy to improve how you anticipate, withstand, and recover from the most advanced cyberattacks. Our Exposure Management services are tailored to your business needs to help your organisation proactively identify gaps and refine your security strategy. LEARN MORE **eSentire Penetration Test** eSentire's Penetration Testing helps you understand how effective your privacy and security controls are, before a malicious actor breaks into your environment, causing business disruption. Our penetration testers use the latest tactics, techniques and procedures (TTPs) in an authorised attempt to gain access to your resources without the knowledge of usernames, passwords, and other usual means of access. In the post-penetration testing report, we provide a detailed summary of high-risk systems and recommendations on how you can improve your security posture. LEARN MORE

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
Digital Operational Resilience Testing	*Article 26: Advanced testing of ICT tools, systems and processes based on TLPT*	**eSentire Exposure Management** eSentire Exposure Management advisory services help you proactively identify gaps in your cybersecurity program, mitigate identified vulnerabilities, reduce your cyber risk, and build a cybersecurity strategy to improve how you anticipate, withstand, and recover from the most advanced cyberattacks. Our Exposure Management services are tailored to your business needs to help your organisation proactively identify gaps and refine your security strategy. LEARN MORE **eSentire Penetration Test** eSentire's Penetration Testing helps you understand how effective your privacy and security controls are, before a malicious actor breaks into your environment, causing business disruption. Our penetration testers use the latest tactics, techniques and procedures (TTPs) in an authorised attempt to gain access to your resources without the knowledge of usernames, passwords, and other usual means of access. In the post-penetration testing report, we provide a detailed summary of high-risk systems and recommendations on how you can improve your security posture. LEARN MORE
	Article 27: Requirements for testers for the carrying out of TLPT	**eSentire Exposure Management** eSentire Exposure Management advisory services help you proactively identify gaps in your cybersecurity program, mitigate identified vulnerabilities, reduce your cyber risk, and build a cybersecurity strategy to improve how you anticipate, withstand, and recover from the most advanced cyberattacks. Our Exposure Management services are tailored to your business needs to help your organisation proactively identify gaps and refine your security strategy. LEARN MORE **eSentire Penetration Test** eSentire's Penetration Testing helps you understand how effective your privacy and security controls are, before a malicious actor breaks into your environment, causing business disruption. Our penetration testers use the latest tactics, techniques and procedures (TTPs) in an authorised attempt to gain access to your resources without the knowledge of usernames, passwords, and other usual means of access. In the post-penetration testing report, we provide a detailed summary of high-risk systems and recommendations on how you can improve your security posture. LEARN MORE

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
Managing of ICT Third-Party Risk	*Article 28: General principles*	**eSentire Virtual CISO (vCISO) - Vendor Risk Management** eSentire's named Virtual CISO (vCISO) works directly with you to establish a process to identify, track, and mitigate third-party and vendor risks to your business. Our experts work with you to assess and review existing vendor due diligence processes and develop a pragmatic Vendor Risk Management Program. To ensure continued cyber resilience against third-party risks, we conduct annual reassessments and reviews of your Vendor Risk Management program to identify opportunities for improvement. LEARN MORE **eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE
	Article 29: Preliminary assessment of ICT concentration risk at entity level	
	Article 30: Key contractual provisions	
	Article 31: Designation of critical ICT third-party service providers	
	Article 32: Structure of the Oversight Framework	
	Article 33: Tasks of the Lead Overseer	
	Article 34: Operational coordination between Lead Overseers	
	Article 35: Powers of the Lead Overseer	
	Article 36: Exercise of the powers of the Lead Overseer outside the Union	
	Article 37: Request for information	
	Article 38: General investigations	
	Article 39: Inspections	
	Article 40: Ongoing oversight	
	Article 41: Harmonisation of conditions enabling the conduct of the oversight activities	
	Article 42: Follow-up by competent authorities	
	Article 43: Oversight fees	
	Article 44: International cooperation	

DORA - Digital Operational Resilience Act (EU) 2022/2554)		eSentire Services
Information-sharing Arrangements	*Article 45: Information-sharing arrangements on cyber threat information and intelligence*	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. LEARN MORE **eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organisation's cybersecurity program and initiatives. LEARN MORE

Ready to get started?

Connect with an eSentire Security Specialist to learn how you can reduce your cyber risks, build resilience, and prevent disruption.

GET STARTED

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSentire