ANOMALI

PLAYBOOK

The DORA Playbook: Your Step-by-Step Guide to Cyber Resilience

Table of Contents

Introduction

The Digital Operational Resilience Act (DORA), a European Union (EU) security regulation, took effect in January 2025.

The act introduced a unified framework to safeguard the financial sector against escalating cyber threats. If your organization has not yet implemented DORA's requirements, it's essential to get started right away.

DORA isn't just about meeting regulatory requirements — it's a blueprint for building long-term operational resilience in the face of an evolving threat landscape. For security operations centre (SOC) and cyber threat intelligence (CTI) teams, this means embracing advanced tools like threat intelligence platforms (TIPs) and Security Information and Event Management (SIEM) to stay ahead of risks, ensure business continuity, and meet the expectations of regulators and stakeholders.

This guide unpacks what DORA means for your organisation and explores how the right technologies can simplify compliance while transforming your approach to threat detection and response.

What is DORA? A Practical Overview

DORA (Digital Operational Resilience Act) is an EU regulation aimed at strengthening the resilience of financial institutions to IT-related disruptions and risks. While DORA is focused on operational resilience, many of its principles align with technical security controls that can be implemented to ensure compliance and improve overall security posture.

DORA serves as a roadmap for strengthening the digital resilience of financial institutions, helping organisations prepare for, withstand, and recover from cyber incidents. Based on the prescriptive chapters of DORA, SOC, and CTI teams will have to address the following five initiatives.

1. Identify and Mitigate Cyber Risks

DORA emphasises the importance of actively identifying vulnerabilities and mitigating risks before they become incidents. This requires establishing robust detection and prevention systems, backed by real-time threat intelligence. SOC and CTI teams will need a proactive approach, using advanced tools to monitor, prioritise, and respond to threats effectively.

2. Ensure Operational Continuity

DORA emphasises maintaining critical services even during disruptions. Beyond a recovery plan, teams must stress-test their operations to ensure resilience against a variety of cyber threats, from ransomware to system failures. DORA pushes organisations to embed continuity into every layer of their operations.

3. Standardise Incident Reporting

DORA introduces a unified approach to incident reporting, ensuring that significant cyber events are reported promptly to regulators. For SOC teams, this means establishing clear protocols to gather, analyse, and share incident data. Accurate and timely reporting not only ensures compliance but also builds trust with regulators and stakeholders.

4. Oversee Third-Party Providers

With many financial entities relying on third-party information and communication technology (ICT) services, DORA enforces stricter oversight of supply chain risks. Organisations must assess vendors' cybersecurity capabilities, monitor their performance, and have contingency plans for potential disruptions. This gives SOC and CTI teams greater visibility into external risks that could impact operations.

5. Conduct Regular Resilience Testing

Resilience isn't a one-off effort. DORA mandates continuous testing of ICT systems to identify vulnerabilities and measure preparedness. These activities, from red team exercises to penetration testing, help teams uncover weaknesses and fine-tune their defences. Regular testing ensures that organisations are always ready to respond to emerging threats.

By enforcing these measures, DORA sets a new baseline for cybersecurity across the financial sector, harmonising practices for all entities — from established banks to cutting-edge financial technology firms. The result? A more secure and resilient financial ecosystem.

Mapping DORA Requirements to Standard Technical Security Controls

ICT Risk Management

- **Asset management:** Maintain an up-to-date inventory of all ICT assets (e.g., CMDBs), along with any potential exposure.
- **Vulnerability management:** Implement vulnerability scanning and patch management systems.
- **Threat intelligence:** Use TIPs to monitor, correlate, and act on emerging threats.
- **Risk assessments:** Conduct regular risk assessments using frameworks like NIST or ISO 27001.

Incident Reporting

- **SIEM:** Deploy SIEM tools to collect and analyse logs for detecting incidents. Matching log data with known threats allows greater accuracy in identifying actual incidents. Ensure you are able to triage and respond to incidents through integrations.
- **Incident response playbooks:** Use automated workflows and playbooks in security orchestration, automation, and response (SOAR) platforms.
- **Logging and monitoring:** Ensure comprehensive logging of all critical systems with retention policies aligned to compliance requirements. Ideally, your data retention (hot) should go back years, not just 90 days.
- **TIP:** Ensure your TIP provides real-time insights into adversaries' tactics, techniques, and procedures (TTPs), equipping teams with the context needed for rapid incident analysis and response. Quick and informed responses minimise the impact of incidents and ensure compliance with DORA's structured reporting requirements. Additionally, use threat intelligence formats such as STIX/TAXII to ensure that incident data is shared in a consistent, machine-readable format. This not only speeds up reporting but also supports collaboration with regulators and peers.

Operational Resilience Testing

- **Penetration testing:** Conduct regular penetration testing to uncover vulnerabilities.
- **Red/blue team exercises:** Simulate attack and defence scenarios to evaluate resilience.
- **Disaster recovery testing:** Test disaster recovery and backup systems on a regular cadence.
- **Chaos engineering:** Regularly use tools to simulate outages and measure system responses.

Third-Party Risk Management

- **Third-party risk assessment tools:** Evaluate the security posture of vendors using platforms and keep your scores above the threshold.
- **Vendor contracts:** Include and enforce clauses mandating service-level agreements (SLAs) for security, incident reporting, and audit rights.
- **Access control:** Limit third-party access using privileged access management (PAM) tools.

Information Sharing

- **TIPs:** Consume and instantly share threat intelligence from trusted sources, both within your internal IT ecosystem and across your broader domain.
- **ISAC memberships:** Join sector-specific information sharing and analysis centres (ISACs).
- **Collaboration tools:** Implement secure tools for cross-organization communication, such as encrypted messaging platforms.

Challenges and Considerations When Integrating Threat Intelligence and Security Analytics for DORA Compliance

While combining threat intelligence with operational telemetry creates a unified defence and supports DORA compliance, the integration comes with specific challenges and considerations. Success requires strategic planning, technical expertise, and a clear focus on operational needs.

Technical Challenges

Integration Complexity

Bridging intelligence and operational platforms may present integration risks, particularly in organisations with diverse systems and environments. Seamless integration demands compatibility between tools and careful coordination of data flows.

- **What to consider:** Organisations must evaluate both platforms for interoperability and ensure they have the necessary APIs, connectors, and support for integration.
- **Why it matters:** Poor integration can lead to data silos and missed or delayed opportunities to correlate critical threat intelligence with internal events.

Data Overload

The combination of intelligence with operations significantly increases the volume of data processed, including logs, alerts, and threat feeds. Without proper filtering and prioritisation, this can overwhelm systems and analysts.

- **What to consider:** Implementing mechanisms to filter irrelevant data and prioritise high-risk threats for action. A TIP can be adept at enhancing and filtering threat data.
- **Why it matters:** Managing the influx of information effectively ensures teams can focus on meaningful insights instead of getting lost in noise.

Scalability

As organisations expand their digital footprints, the volume of data generated by intelligence and operational teams will increase. Ensuring that the integrated solution can scale to meet these demands is critical.

- **What to consider:** Choose platforms that can handle expanding data volumes and allow for future growth without performance degradation. Cloud-native solutions were built from the ground up specifically for this scenario.
- **Why it matters:** Scalability ensures the solution remains effective as the organisation evolves and faces more complex threats.

Operational Considerations

Skills Gaps

Using an integrated intelligence and operational solution effectively requires skilled personnel who can interpret data, identify patterns, and take timely action. A lack of expertise can limit the solution's effectiveness.

- **What to consider:** Invest in training and upskilling SOC and CTI teams to maximise the value of the integrated solution.
- **Why it matters:** Well-trained teams ensure the system's capabilities are fully used, leading to stronger compliance and threat response.

Cost Management

The initial investment in CTI and SIEM platforms, along with ongoing operational costs, can be significant, particularly for smaller organisations.

- **What to consider:** Assess the total cost of ownership, including licenses, infrastructure, and training, to ensure the investment aligns with organisational budgets.
- **Why it matters:** Effective cost management ensures long-term sustainability of the solution while delivering value.

Vendor Selection

Selecting the right vendors for CTI and SIEM is essential to achieve smooth integration and ensure the solution meets the organisation's needs.

- **What to consider:** Look for vendors with domain expertise, proven compatibility, strong support services, a wide partner ecosystem, and features tailored to financial services.
- **Why it matters:** The right vendors reduce integration complexity and enhance the overall effectiveness of the solution.

Integrating intelligence and operational solutions is a strategic move that supports DORA compliance and strengthens cybersecurity. However, addressing these technical and operational challenges head on is essential for success. By carefully planning for integration, scalability, and resource needs, organisations can unlock the full potential of a unified approach.

Achieving DORA Compliance with Anomali

As financial institutions navigate the complexities of DORA compliance, they need a solution purpose-built to address these challenges. That's where Anomali excels. From the ground up, Anomali has been designed to tackle the toughest issues in threat intelligence and security operations, empowering organisations to meet regulatory requirements and strengthen their resilience.

Anomali delivers the most comprehensive security platform available for DORA compliance. Only Anomali provides AI-Powered threat intelligence with a modern approach to SIEM in one unified platform. It simplifies compliance, enhances threat detection, and ensures operational resilience.

Next, we'll explore how Anomali addresses the critical components of DORA, equipping financial institutions to stay ahead of today's regulatory demands and tomorrow's evolving threats.

Anomali ThreatStream: A Critical Partner in DORA Compliance

ICT risk management is about understanding threats and how they may impact your unique environment. In this scenario, threat intelligence, asset management, and vulnerability management all come into play. Anomali ThreatStream allows you to not only gather intel from hundreds of sources but to also deduplicate, score, rank, and prioritise it by incorporating contextual details about your environment (such as geography, industry, asset context, and vulnerabilities). This customisation leads to a better understanding of how threats may affect you.

Anomali ThreatStream empowers financial institutions to stay ahead of evolving cyber threats by delivering actionable intelligence that drives proactive security measures. Designed to address the demands of modern regulatory frameworks like DORA, ThreatStream equips organisations with the tools to identify risks, respond to incidents, and strengthen their cybersecurity posture with precision and efficiency.

Risk Identification and Assessment

ThreatStream gathers and analyses intelligence from diverse sources, such as open source intelligence (OSINT), dark web monitoring, and vendor feeds. This broad view allows CTI teams to uncover emerging threats, vulnerabilities, and patterns of malicious activity.

- **Why this matters for DORA:** Proactively identifying risks aligns with DORA's emphasis on preventing incidents before they occur. With ThreatStream, organisations can anticipate attacks and implement targeted defences that reduce potential disruptions.
- **ThreatStream in action:** Spotting trends — such as a surge in phishing campaigns or identifying vulnerable software versions that adversaries are targeting — enables preemptive action.

Third-Party Risk Management

Financial institutions rely heavily on third-party ICT providers, and ThreatStream plays a critical role in managing the risks they pose. By analysing vendor vulnerabilities, breach history, and threat profiles, ThreatStream gives organisations a clearer picture of their supply chain risks.

- **Why this matters for DORA:** DORA mandates strict oversight of third-party ICT providers, and ThreatStream gives organisations the insights they need to assess, monitor, and mitigate these risks.
- **ThreatStream in action:** CTI teams can flag vendors with a history of breaches or alert decision-makers to supply chain risks, enabling informed choices about partnerships and risk management strategies.

Threat Hunting and Continuous Improvement

ThreatStream enables proactive threat hunting by analysing both historical data and real-time intelligence. This approach uncovers hidden risks and informs long-term improvements in cybersecurity defences.

- **Why this matters for DORA:** DORA requires organisations to build resilience against evolving threats. ThreatStream supports this by continuously refining detection capabilities and security postures.
- **ThreatStream in action:** Analysing trends in ransomware attacks or identifying the most exploited vulnerabilities helps guide updates to security measures, keeping the organisation ahead of attackers.

Operational Benefits of ThreatStream

The value of Anomali's platform goes beyond compliance — it transforms how organisations manage cybersecurity risks and respond to threats. Below are the key operational benefits that Anomali brings to financial institutions.

Enhanced Situational Awareness

ThreatStream offers a holistic view of the threat landscape by analysing data from a variety of sources, such as global attack trends, emerging vulnerabilities, and adversary behaviours. This comprehensive intelligence equips CTI teams with the insights needed to make proactive, informed decisions.

- **Why it matters:** Understanding the full scope of threats helps prioritise actions, reduce blind spots, and allocate resources effectively.
- **ThreatStream in action:** Monitoring a surge in ransomware attacks targeting specific industries can prompt a review of defences, ensuring critical assets are protected.

Improved Collaboration

By sharing structured threat intelligence, CTI teams foster stronger collaboration between financial institutions, regulatory bodies, and industry peers. Formats like STIX/TAXII allow intelligence to be easily exchanged and acted upon.

- **Why it matters:** Sharing insights creates a unified defence, enabling financial entities to collectively respond to industry-wide threats. This collaborative approach also strengthens relationships with regulators by demonstrating a proactive commitment to cybersecurity.
- **ThreatStream in action:** Sharing intelligence on an active phishing campaign targeting the financial sector helps peers and regulators prepare and respond effectively, reducing the overall impact.

Resource Optimisation

Anomali automates the processing of vast amounts of threat data, turning raw information into actionable insights. This automation reduces the workload for CTI analysts, allowing them to focus on more strategic tasks.

- **Why it matters:** Automation enhances efficiency and ensures that analysts have the bandwidth to investigate complex threats and refine security strategies.
- **ThreatStream in action:** Automating the detection of indicators of compromise (IoCs) frees analysts to conduct deeper investigations into adversary behaviours, improving overall security outcomes.

By enhancing situational awareness, fostering collaboration, and optimising resources, Anomali empowers financial institutions to stay resilient and adaptive. For CTI teams, these benefits underscore the critical role they play in strengthening their organisations against a constantly evolving threat landscape.

Anomali Security Analytics: The SOC Team's Ally in DORA Compliance

For SOC teams, a robust SIEM platform, such as Anomali's Security Analytics, is essential for meeting DORA's requirements while enhancing the organisation's overall security posture. Acting as the nerve centre of an organisation's cybersecurity operations, Anomali Security Analytics provides the tools needed to monitor, analyse, and respond to security events in real time.

Continuous Monitoring and Detection

Anomali collects and analyses logs from a wide range of sources — network devices, servers, applications, and more. This centralised approach enables SOC teams to detect anomalies and potential threats quickly and efficiently.

- **Why this matters for DORA:** Continuous monitoring aligns with DORA's focus on proactive risk management, ensuring organisations can identify and mitigate threats before they escalate.
- **Security Analytics in action:** Anomali uses machine learning (ML) to spot patterns that indicate malicious activity, such as unusual login attempts or data exfiltration, helping teams act decisively to neutralise risks.

Incident Reporting and Documentation

With Anomali Security Analytics, SOC teams can streamline incident reporting by automatically generating detailed reports on the nature, scope, and impact of security events. These reports are essential for demonstrating compliance with DORA's structured reporting requirements.

- **Why this matters for DORA:** Timely and accurate reporting helps organisations meet regulatory deadlines and improve transparency with authorities.
- **Security Analytics in action:** During a ransomware attack, Security Analytics can provide a comprehensive incident report within minutes, ensuring regulators receive critical information quickly and in the required format.

Integration with ThreatStream

Integrating Security Analytics with ThreatStream enhances detection capabilities by correlating internal telemetry with external threat intelligence. This combined approach provides deeper context and faster threat identification.

- **Why this matters for DORA:** Real-time integration supports the identification of sector-specific or geography-specific threats, helping organisations stay ahead of targeted attacks.
- **Security Analytics in action:** When ThreatStream flags a phishing campaign targeting the financial sector, Security Analytics can correlate this intelligence with internal email activity to identify and block malicious attempts.

Third-Party Risk Monitoring

Security Analytics can also monitor activity related to third-party vendors, providing visibility into potential risks associated with external ICT service providers. This ensures compliance with DORA's requirements for third-party risk oversight.

- **Why this matters for DORA:** Financial institutions need to demonstrate control over third-party risks, and Security Analytics helps track vendor activity for unusual behaviours or vulnerabilities.
- **Security Analytics in action:** Monitoring vendor logins for unusual access times or geolocations allows SOC teams to respond swiftly to potential breaches stemming from third-party relationships.

Operational Benefits of Anomali Security Analytics

Security Analytics delivers critical advantages that go beyond threat detection, empowering SOC teams to work smarter, respond faster, and maintain regulatory compliance.

Centralised Visibility

Security Analytics aggregates logs and data from across the organisation, creating a unified view of all security events. This centralisation eliminates silos and reduces blind spots, giving SOC teams the insights needed to make informed decisions.

- **Why it matters:** A comprehensive view of the organisation's security landscape ensures no threat goes unnoticed, enabling proactive defence.
- **Security Analytics in action:** SOC teams can detect unusual login patterns across departments and geographies in a single dashboard, instead of analysing disconnected logs manually.

Improved Incident Response

With real-time alerts and automated workflows, Anomali empowers SOC teams to swiftly contain and remediate threats. Automating routine tasks reduces response times and minimises the impact of incidents.

- **Why it matters:** Faster response times mean less disruption to critical operations, ensuring the organisation remains resilient in the face of attacks.
- **Security Analytics in action:** When Security Analytics flags a malware outbreak, automated workflows can isolate affected endpoints and alert analysts, enabling immediate containment.

Simplified Regulatory Alignment

Security operations (SecOps) platforms often come with pre-built compliance templates designed to meet regulatory requirements, including DORA. These templates simplify reporting and ensure that SOC teams consistently meet compliance standards without reinventing the wheel.

- **Why it matters:** Streamlined compliance reduces the burden on SOC teams and ensures organisations stay ahead of regulatory deadlines.
- **Security Analytics in action:** Pre-configured templates generate DORA-compliant incident reports automatically, saving time and ensuring alignment with regulatory expectations.

For SOC teams, SecOps platforms like Anomali's are more than just a powerful tool — they are strategic assets. By providing centralised visibility, enhancing incident response, and simplifying compliance, Anomali's Security Operations Platform enables organisations to stay secure, resilient, and ready to meet the DORA challenge.

ThreatStream and Security Analytics: A Powerful Alliance for DORA Compliance

Anomali ThreatStream and Security Analytics are powerful tools on their own, but they work together in the Anomali Security and IT Operations Platform to strengthen compliance and cybersecurity. With this unified approach, organisations can streamline operations, enhance threat detection, and meet DORA's requirements more effectively.

Data Correlation

Through Anomali's integrated platform, internal logs from Security Analytics are enriched with external intelligence from ThreatStream. This integration uncovers sophisticated attack patterns and their potential consequences that might otherwise go unnoticed.

- **Why it matters:** Combining internal and external data allows teams to detect and contextualise advanced threats earlier, reducing the likelihood of significant disruptions.
- **Anomali in action:** Security Analytics can flag a suspicious login attempt, while ThreatStream correlates this data with known adversary tactics, confirming it as part of a larger attack campaign.

Incident Prioritisation

ThreatStream provides critical context about the severity and relevance of detected threats. This enables Security Analytics to rank incidents based on their potential impact, ensuring that teams focus on the highest risks first.

- **Why it matters:** Prioritising threats saves time and ensures resources are allocated to the most pressing issues, aligning with DORA's emphasis on proactive risk management.
- **Anomali in action:** A detected phishing attempt targeting a C-suite executive is flagged as high-priority after ThreatStream uncovers its association with a known ransomware group.

Automated Workflows

Integrating ThreatStream intelligence with Security Analytics operational data enables automated responses to specific threat scenarios, reducing response times and limiting damage. Actions — such as isolating affected systems or blocking malicious IP addresses — can be triggered instantly.

- **Why it matters:** Automation reduces the burden on teams, speeds up containment, and ensures consistent responses to threats.
- **Anomali in action:** When a ThreatStream feed identifies a malicious IP address, Security Analytics automatically blocks it across the network, preventing further intrusion.

Enhanced Reporting

As a fully integrated Security and IT Operations Platform, Anomali ThreatStream and Security Analytics provide comprehensive reporting capabilities that combine internal telemetry with external threat intelligence. This ensures that compliance documentation meets DORA’s requirements while also providing deeper insights.

- **Why it matters:** Unified reporting simplifies regulatory submissions and improves transparency for regulators, showcasing an organisation’s readiness and resilience.
- **Anomali in action:** A DORA-compliant incident report includes both the technical details of an internal breach and external intelligence linking the incident to a larger threat group.

Real-World Example: The Power of Integration

A financial institution detected unusual activity on its network using Anomali Security Analytics. By integrating this data with insights from Anomali ThreatStream, the organisation quickly identified the activity as part of a ransomware campaign specifically targeting the financial sector.

With automated workflows in place, ThreatStream instantly isolated the affected systems, notified relevant stakeholders, and generated a detailed compliance report for regulatory authorities — all within minutes.

This seamless integration highlights how CTI and SOC teams working together can enhance both response efficiency and regulatory compliance, turning a potential crisis into a controlled outcome.

Achieve DORA Compliance with the Anomali AI-Powered Security and IT Operations Platform

Anomali's Security and IT Operations Platform helps financial institutions achieve compliance by integrating threat intelligence/CTI with Security Analytics/ SIEM capabilities tailored to meet DORA's specific requirements.

Proactive Risk Management

- **How:** The Anomali Security and IT Operations Platform enables financial institutions to proactively identify, assess, and mitigate cyber risks. It enhances and contextualises real-time threat intelligence, integrating with Anomali's Security Analytics to deliver incident and threat relevance to internal telemetry. Anomali's Generative AI Copilot enables the platform to deliver advanced analytics with unprecedented speed.
- **DORA alignment:** This supports DORA's emphasis on proactive risk identification and management, ensuring organisations can anticipate and prevent incidents. The use of enriched threat intelligence provides an actionable framework that threat hunters can leverage to anticipate and mitigate threats.

Continuous Monitoring and Threat Detection

- **How:** Anomali correlates internal security data with enriched, contextualised threat intelligence from a broad range of sources (OSINT, commercial, and premium feeds) to detect sophisticated attack patterns and anomalies. Its lookback capability is measured in years and searched in seconds (not weeks and hours or days, like most competing offerings).
- **DORA alignment:** This aligns with the regulation's requirement for continuous monitoring of ICT systems to detect, prevent, and respond to threats. The main advantage of Anomali's approach is the ability to run monitoring and detection in seconds.

Streamlined Incident Reporting

- **How:** The Anomali Security and IT Operations Platform generates automated reports that include detailed information on incidents, enriched with threat intelligence for added context. These reports seamlessly correlate internal telemetry with external threat data, delivering comprehensive summaries at both the technical and business levels — all within seconds.
- **DORA alignment:** These reports simplify compliance with DORA's structured incident reporting requirements, ensuring immediate, accurate communication with regulators, operators, and executive management.

Third-Party Risk Oversight

- **How:** Anomali ThreatStream enables institutions to assess and monitor third-party vendors by identifying their services' vulnerabilities, breaches, and risks.
- **DORA alignment:** This helps organisations meet DORA's mandate to oversee and manage risks from external ICT providers.

Scalability for Growing Threat Landscapes

- **How:** The cloud-native platform is built to scale with organisational needs, ensuring it can handle increasing data volumes as financial institutions expand their digital footprints.
- **DORA alignment:** Supports DORA's demand for resilient ICT systems capable of managing a growing, evolving threat landscape.

Unified CTI and SIEM Integration

- **How:** Anomali's integration of ThreatStream intelligence with Security Analytics' telemetry data enables financial institutions to benefit from seamless data correlation, prioritisation, and automated workflows.
- **DORA alignment:** This unified approach ensures compliance while enhancing overall operational efficiency and security posture.

By combining advanced threat intelligence, automation, and scalability, Anomali not only helps financial institutions meet DORA requirements but also strengthens their resilience against emerging threats. This positions organisations to thrive in the regulatory environment while staying ahead in the cybersecurity landscape.

Get Started with Anomali

DORA is more than just a regulatory requirement — it's a chance to build a stronger, more resilient financial institution.

By uniting the capabilities of threat intelligence with security operations, you can transform your organisation's approach to cybersecurity and stay ahead of ever-evolving threats.

This journey requires careful planning, the right tools, and a commitment to collaborating across teams. The challenges may be significant, but the rewards are even greater:

- **Enhanced operational resilience** to ensure business continuity during disruptions.
- **Improved threat detection** to stay ahead of evolving cyber risks.
- **Confidence in being prepared** for the unexpected, no matter how the threat landscape evolves.

Now is a great time to assess your current capabilities, identify gaps, and explore how a unified strategy leveraging the integration of threat intelligence with SecOps can help your organisation thrive. Consider your current capabilities, identify gaps, and build a unified strategy that leverages threat intelligence and operational data to their full potential. The sooner you begin, the better prepared your organisation will be, both for DORA and for the future of cybersecurity.

The Clear Choice for Modern Security Operations

Anomali's Security and IT Operations Platform is the perfect solution to help your team prepare for DORA compliance. Anomali combines ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one easy-to-use solution at a fraction of the cost of competing offerings.

Innovative, Effective Technology

Cybersecurity solutions for organisations of all sizes. AI-Powered intelligence-driven solutions for a more secure world. That's Anomali.

Discover how Anomali can help you create a robust, highly adaptive security solution. Schedule a demo of Anomali's Security and IT Operations Platform to see why it's different and how it can transform your organisation's security posture.

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI