DARKTRACE

Ultimate Guide

Incident Response in AWS

Abstract

Amazon Web Services (AWS) is one of the largest Cloud Service Providers (CSPs) globally, with over 200 services available. However, this vast ecosystem introduces significant challenges for security and incident response. The huge range of services, diverse logging formats, and dynamic nature of cloud environments can complicate the identification and management of security incidents.

The threat landscape for cloud environments has evolved alongside AWS's capabilities. Organizations now face sophisticated attacks such as ransomware, data exfiltration, privilege escalation, and supply chain compromises. These threats emphasize the critical need for a proactive and well-structured approach to incident response.

This guide aims to empower security teams to address incidents in the cloud effectively by covering:

- An overview of key AWS services and log sources relevant to incident response, including AWS CloudTrail, AWS CloudWatch, and Virtual Private Cloud (VPC) Flow Logs.
- Strategies for responding to incidents in services such as EC2, EKS, ECS, Lambda, and S3.
- Best practices for automating incident evidence collection and analysis to reduce response times and improve accuracy.
- Guidance on forensic analysis tailored to the complexities of AWS environments.
- Strategies for addressing challenges such as data volatility, cross-account operations, and multi-cloud complexity.

Contents

04 Key AWS log sources

05 Service-specific incident response strategies

09 Automating incident response

11 Forensic analysis in AWS

12 Post-incident review and continuous improvement

13 Addressing common challenges in AWS incident response

14 Tools and resources

16 Conclusion and recommendations

Key AWS log sources

Incident response in AWS relies heavily on the ability to collect, analyze, and act on log data. AWS offers a variety of logging services, each with different use cases. Understanding these log sources and their capabilities is crucial for building a strong foundation for incident detection and response. Below are the key AWS log sources that security teams should prioritize:

AWS CloudTrail Logs

AWS CloudTrail provides a detailed record of API calls made within an AWS account. It captures information such as the identity of the caller, the time of the call, and the parameters used. These logs are indispensable for auditing account activity and investigating potential security incidents.

Best practices include:

- Enabling CloudTrail for all regions.
- Configuring logs to be delivered to a secure Simple Storage Service (S3) bucket.
- Using AWS CloudTrail Insights for anomaly detection.

AWS CloudWatch Logs

AWS CloudWatch collects and monitors logs from various AWS services and custom applications. It allows security teams to create metrics, set alarms, and perform detailed log analysis.

Key tips include:

- Centralizing logs from multiple sources into CloudWatch.
- Leveraging Log Insights for querying and visualizing log data.
- Setting up alarms to monitor unusual activity in real time.

VPC Flow Logs

VPC Flow Logs capture network traffic within an AWS VPC. These logs provide insights into accepted and rejected connections, making them invaluable for identifying unusual network behavior or potential breaches.

Recommendations include:

- Enabling VPC Flow Logs for all critical subnets.
- Integrating flow logs with CloudWatch or an external SIEM for analysis.

S3 access logs

S3 access logs record operations performed on S3 buckets and objects. They are essential for tracking data access and modifications.

Best practices include:

- Enabling access logging for all sensitive buckets.
- Reviewing logs regularly to detect unauthorized access.
- Using automated tools to parse and analyze logs at scale.

Other logging sources

Other AWS services, such as Elastic Load Balancing (ELB) and AWS Web Application Firewall (WAF), also provide valuable logging capabilities.

Security teams should:

- Enable access logs for ELB to track request and response data.
- Use AWS WAF logs to monitor and block malicious web traffic.

By configuring and leveraging these log sources effectively, organizations can enhance their ability to detect, analyze, and respond to security incidents in AWS environments.

Service-specific incident response strategies

AWS environments consist of multiple different services, each presenting unique challenges for incident response. Below are detailed strategies tailored to specific AWS services:

Elastic Compute Cloud (EC2)

- **Quarantine** - modify the security group of the affected instance to block all inbound and outbound traffic.
- **Snapshot** - take snapshots of all attached Elastic Block Storage (EBS) volumes for forensic analysis.
- **Investigate IAM** - review the instance's role and permissions in CloudTrail logs to identify potential misuse.
- **Automate** - Use AWS Systems Manager (SSM) to execute incident response commands directly on the compromised instance.

Resources

- SANS has a white paper on Digital Forensic Analysis of Amazon Linux EC2 Instances and provides the free SANS SIFT Linux distribution that can be used for command-line analysis of acquired EC2 instances at the raw disk level.

AWS provides a number of solutions to help isolate, preserve, and analyze compromised EC2 systems. A few key ones to play with include:

- **Solution for AWS Cloud for incident response in EC2 instances** - this is a CloudFormation deployment to quarantine EC2 systems via SSM commands on the host themselves, perform security group changes, and snapshot EBS volumes.
- **Automated incident response with SSM** - another solution that uses SSM that can also quarantine EC2 systems, but is based on the outcome of GuardDuty events.
- **Automated incident response and forensics framework** - a set of Security Hub actions to acquire data from EC2 systems.
- **Automated Forensics Orchestrator for Amazon EC2** - a CloudFormation deployment to acquire data from EC2 systems.
- **EC2 auto clean room forensics** - a CloudFormation deployment that will run the open-source fls tool to dump file timestamps from files found on a compromised EC2 system.

Elastic Kubernetes Service (EKS)

While the visibility provided by built-in CSP tools (e.g. AWS CloudWatch and CloudTrail) is important, these data sources alone are not sufficient to perform an in-depth investigation. Leveraging third-party incident and threat intelligence capabilities proves vital in gaining a deeper level of visibility across container assets. In this context, the useful data to include as part of your investigation are the system logs and files from within the container, the container's running processes and active network connections, the container host system and container runtime logs (if accessible), the container host memory (if accessible), and the AWS VPC flow logs for the VPC the container is attached to. If data collection wasn't baked into the container declaration before the need to investigate arose, you need to rely on data you can actively interrogate out of the container.

Important note

If the container is running on an underlying EC2, then refer to the suggested steps above for immediate action. If the container is running on Fargate, then collect any data required for later analysis before subsequently suspending it.

- **Log collection** - capture Kubernetes API server logs, audit logs, and application logs in CloudWatch.
- **Data preservation** - use kube-forensics to extract data from affected pods before termination.
- **Containment** - isolate compromised pods or nodes to prevent lateral movement within the cluster.
- **GuardDuty integration** - leverage EKS-specific findings for early threat detection.

Resources

- kube-forensics allows a cluster administrator to dump the current state of a running pod and all its containers so that security professionals can perform offline forensic analysis.
- AWS provides advice on incident response and forensics in its EKS Best Practices documentation on Github. It also recently released new GuardDuty detections for EKS.

Elastic Container Service (ECS) and Fargate

If you're using ECS on Fargate, taking an image of the running container or the container host isn't an option as the underlying AWS infrastructure is shared with no access to the end customers. In this case, the /proc directory gives us a snapshot of the volatile state of the container, much like a memory dump. Using this 'snapshot' we can build a basic picture of what is going on in the container at that time, such as running processes, active network connections, open files, etc. This data provides a foundation of what you need to correlate with other data sources such as firewall logs, network subnet flows, etc. during an investigation to understand the actions carried out by an attacker.

- **Visibility** - collect system logs, running processes, and active network connections using CloudWatch Logs.
- **Data snapshot** - in Fargate environments, access the /proc directory to capture the container's volatile state.
- **Response** - use AWS WAF to block suspicious IP addresses interacting with ECS services.

Lambda

- **Logs and code** - collect CloudWatch logs and preserve all versions of the Lambda function's code.
- **Analysis** - review environment variables for suspicious activity.
- **Containment** - disable triggers temporarily to prevent further execution of the compromised function.

Resources

- AWS provides documentation in investigating Lambda functions:
  - Accessing Amazon CloudWatch logs for AWS Lambda
  - Security in AWS Lambda

S3

- **Access logs** - analyze S3 access logs to identify unauthorized access attempts.
- **Permissions** - review and tighten bucket policies to ensure least-privilege access.
- **Containment** - use Object Lock to enforce write-once-readmany (WORM) protection for critical data.

Elastic Container Registry (ECR)

- **Image scanning** - regularly scan images for vulnerabilities and malware using ECR image scanning or third-party tools.
- **Access control** - review and tighten ECR policies to restrict access to sensitive images.
- **Image integrity** - implement image signing and verification to ensure the integrity of images deployed to EKS or ECS.
- **Incident response** -
  - If a compromised image is identified, quarantine it to prevent further usage.
  - Investigate the source of the compromise and analyze the affected image for malicious code.
  - Rebuild and redeploy applications using clean and verified images.

Other resources

IAM

AWS IAM underpins all other services, enabling and controlling access. It is likely that any non-trivial investigation in AWS will involve IAM.

- Logging IAM and AWS STS API calls with AWS CloudTrail (AWS)
- AWS, IAM Your Father (Part II - Defensive) (AllThingsDFIR)

CloudTrail

While AWS logs to a number of places, CloudTrail is the key platform to become familiar with first.

- Investigating CloudTrail Logs (Medium)
- AWS CloudTrail —Searching Event logs in S3, Athena and Cloudwatch

Training

There are a number of training courses for responding to incidents in AWS, both free and paid.

- Incident Response with AWS Console and CLI (WellArchitetedLabs)
- EC2 DFIR Workshop (Forensicate.cloud)
- Enterprise Cloud Forensics and Incident Response (SANS)

Automating incident response

Automating the collection of incident evidence immediately following detection helps ensure security events are appropriately handled before they are at risk of escalating. The lack of automation coupled with alert fatigue often means things are missed and what may seem like a low-severity detection, may actually be connected to something far more malicious. Leveraging automation to remove many of the complexities and manual steps in kicking off a more thorough investigation means security teams can dive deep more often and better protect their environments. By automating evidence collection, analysts save days and in some cases, even weeks during an investigation.

Below are key aspects and tools for automating incident response:

Automating evidence collection

- **Use** AWS Lambda functions triggered by GuardDuty or CloudWatch alarms to automate the collection of evidence, such as snapshots, logs, and metadata.
- **Configure** EventBridge rules to initiate workflows for common security events, such as unauthorized access or anomalous network traffic.

Integrating with SOAR platforms

- **Integrate** AWS services with Security Orchestration, Automation, and Response (SOAR) platforms.
- **Leverage** these platforms to create playbooks that streamline investigation, containment, and recovery workflows.

Utilizing AWS-specific tools

- **AWS SSM** - automate remediation steps, such as isolating compromised instances or patching vulnerabilities.
- **AWS Security Hub** - aggregate security findings across AWS services and trigger automated responses.
- **Amazon Detective** - investigate incidents faster with automated correlation of log data and visualizations.

Continuous monitoring and response

- **Implement** GuardDuty to provide continuous threat detection and initiate automated responses.
- **Use** CloudWatch and EventBridge to continuously monitor for suspicious activity and execute predefined actions.

Benefits of automation

- **Speed** - respond to incidents in real time, minimizing the potential impact.
- **Scalability** - manage responses across multi-account and multi-region environments effortlessly.
- **Consistency** - ensure standardized processes are followed, reducing human error.

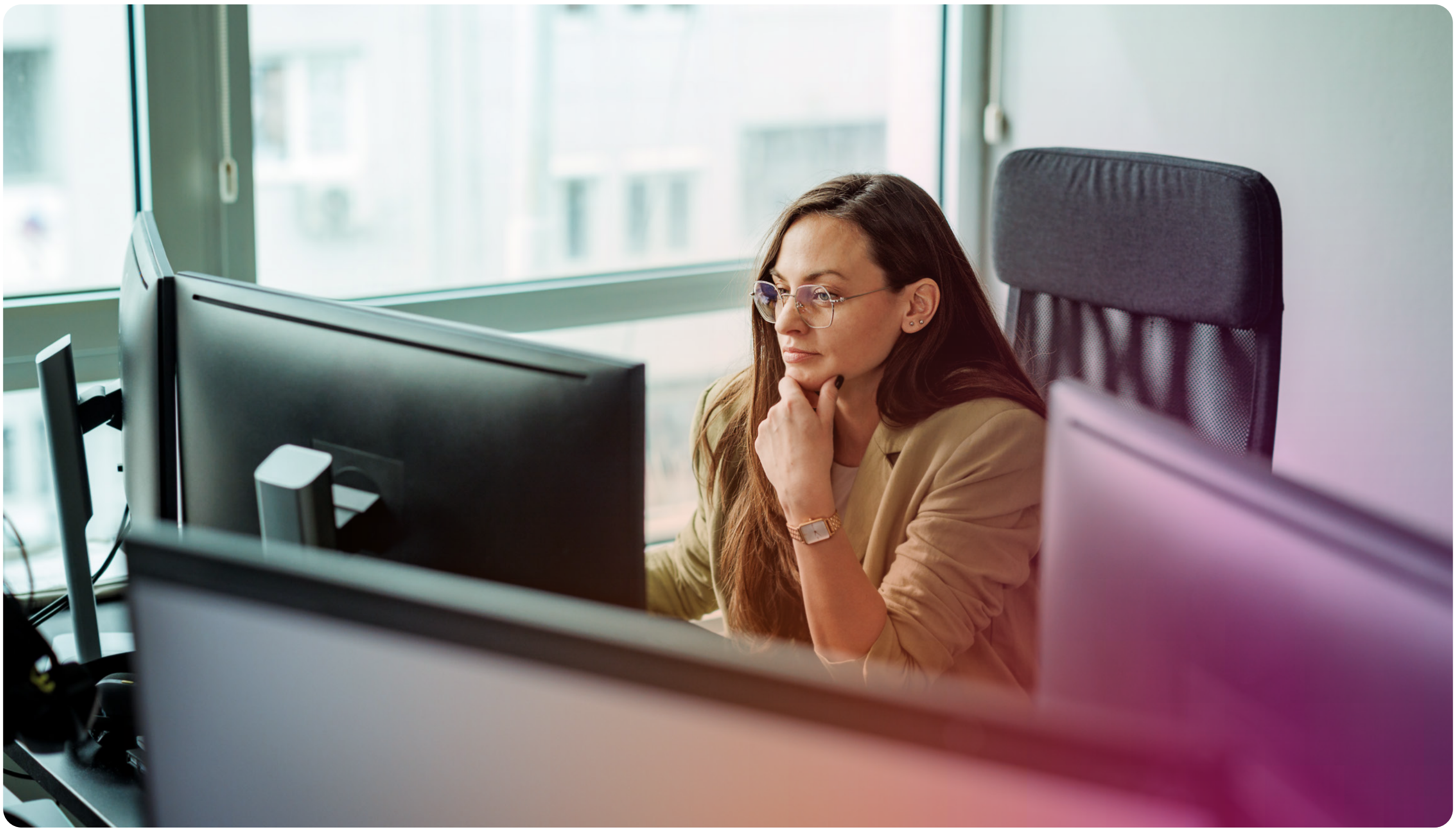
By automating key aspects of incident response, organizations can improve their overall security posture while freeing up security teams to focus on complex investigations and strategic initiatives.

Official AWS resources

AWS provides a number of tools that may be useful when automating response to security incidents:

- EventBridge is a serverless event bus that makes it easy to connect applications together with data from your own applications, integrated Software-as-a-Service (SaaS) applications, and AWS services.
- Lambda can automatically run code in response to events, making it a great choice for event-driven applications.
- Incident Manager is a new capability of AWS Systems Manager to track incidents in AWS as they progress.
- SSM allows you to execute isolation commands directly on EC2 systems from the inside.
- Security Hub aggregates a number of different AWS security tools like Amazon Detective together.
- Standard AWS APIs allow you to change a security group to quarantine a system, for example.

AWS provides documentation, a video, and a white paper which can help pad out incident response plans.



Forensic analysis in AWS

Forensic analysis is critical for understanding the root cause of incidents and determining their scope. The cloud introduces unique challenges and opportunities for forensic investigations, requiring tailored approaches and tools. Below are some key components to consider:

Data collection

- **Preservation** - ensure that evidence is preserved in its original state by taking snapshots of affected resources, such as EBS volumes or RDS instances.
- **Logs** - collect logs from CloudTrail, CloudWatch, and VPC Flow Logs to reconstruct the sequence of events.
- **Memory** - use memory-capture tools to analyze the volatile state of instances or containers when applicable.
- **Artifacts** - focus on collecting the most relevant artifacts based on the suspected attack vector, such as IAM policies, access keys, or application logs.

Data analysis

- **Timelines** - create detailed timelines of events by correlating log data and system activity. Tools like AWS Detective can assist in automating this process. And AWS Athena can be used for log analysis.
- **Indicators of Compromise (IoCs)** - search for IoCs, such as unusual API calls, unauthorized logins, or privilege escalations.
- **Anomaly detection** - use services like GuardDuty or machine learning models to identify deviations from baseline behavior.

EBS volume forensics

- **Snapshot analysis** - perform a detailed analysis of EBS snapshots by mounting them to a forensic workstation or using tools like SIFT Workstation.
- **Data extraction** - extract critical files, logs, and binaries for further investigation.
- **Format conversion** - convert raw disk images into forensic-friendly formats like E01 for long-term analysis.

Network forensics

- **Flow logs** - use VPC Flow Logs to identify unusual traffic patterns, such as data exfiltration or lateral movement.
- **Packet capture -** when possible, capture packets using services like AWS Traffic Mirroring for deeper analysis.
- **Correlation** - correlate network activity with application logs to uncover attacker behavior.

Post-incident reporting

- **Findings** - document the root cause, attack vector, and impact of the incident.
- **Recommendations** - provide actionable recommendations to address vulnerabilities and prevent future incidents.
- **Compliance** - ensure that reports meet legal and regulatory requirements, such as GDPR or HIPAA.

Post-incident review and continuous improvement

A thorough post-incident review is essential for improving the organization’s security posture and refining the incident response process. Each incident provides an opportunity to learn and evolve the organization’s capabilities. Below are the key steps to conducting an effective post-incident review:

Incident summary

- **Document** the sequence of events, including the initial detection, response actions, and resolution timeline.
- **Highlight** the root cause of the incident and contributing factors.

Evaluate response effectiveness

- **Assess** whether detection, containment, and remediation steps were executed efficiently.
- **Identify** delays or missteps that occurred during the response process.

Update policies and procedures

- **Revise** incident response plans based on lessons learned.
- **Update** security controls, configurations, or monitoring rules to prevent similar incidents in the future.

It’s also important to test updates to changes in policies and procedures, to ensure they have both the intended effects and no unintended side effects.

Enhance training and awareness

- **Conduct** training sessions to address gaps in knowledge or skills observed during the incident.
- **Share** lessons learned across the organization to improve awareness.

Leverage insights for continuous improvement

- **Implement** feedback loops to ensure ongoing refinement of incident response capabilities.
- **Use** metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to measure improvements over time.

Compliance and reporting

- **Ensure** that the incident and its resolution are documented in compliance with regulatory requirements.
- **Provide** stakeholders and authorities with a clear and transparent report of the incident and mitigation steps.

Addressing common challenges in AWS incident response

Despite the tools and strategies available, organizations face unique challenges when managing incident response in AWS. Below are some common challenges and ways to address them:

Data volatility

Challenge

AWS resources are dynamic, with instances and containers being spun up or terminated frequently, potentially leading to the loss of critical evidence.

Solution

Implement automated evidence collection workflows triggered by detection tools like GuardDuty and CloudWatch alarms. Use snapshotting and log archival to preserve data.

Multi-account environments

Challenge

Large organizations often manage multiple AWS accounts, complicating visibility and response efforts.

Solution

Centralize monitoring and response using tools like AWS Organizations, Security Hub, and CloudTrail Lake. Ensure cross-account roles are configured for seamless access.

Limited forensic capabilities in cloud-native services

Challenge

Some AWS services, like Lambda and Fargate, offer limited access to underlying infrastructure, making forensic analysis difficult.

Solution

Focus on collecting logs, snapshots, and API data available at the service level. Use tools like Amazon Detective for advanced analysis.

Cross-region considerations

Challenge

AWS services can span multiple regions, complicating incident response efforts.

Solution

Use global services like CloudTrail and GuardDuty, and replicate log data to centralized locations for analysis.

Human error and misconfigurations

Challenge

Misconfigurations, such as open S3 buckets or overly permissive IAM policies, are common entry points for attackers.

Solution

Use AWS Config and Trusted Advisor to identify and remediate misconfigurations proactively. Implement automated guardrails to enforce compliance.

Alert fatigue

Challenge

Security teams often face an overwhelming number of alerts, leading to delayed or missed responses.

Solution

Prioritize alerts using severity levels and correlation tools. Implement automated triage systems to reduce manual workloads.

Tools and resources

A comprehensive incident response strategy in AWS benefits greatly from the use of tools and resources designed to enhance detection, investigation, and remediation. Below are essential community and official AWS tools, along with training opportunities and instructional resources.

Official AWS tools

AWS Security Hub

A centralized service for managing security alerts and compliance checks across AWS accounts.

More information:

AWS Security Hub Documentation →

Amazon Detective

Simplifies root cause analysis by automatically correlating log and event data.

More information:

Amazon Detective Documentation →

AWS CloudTrail

Provides detailed logs of API activity to support auditing and investigations.

More information:

CloudTrail Documentation →

AWS Athena

Interactive analytics service that provides a simplified and flexible way to analyze data.

More information:

Athena Documentation →

GuardDuty

Detects threats using anomaly detection and threat intelligence.

More information:

GuardDuty Documentation →

Community tools

SANS SIFT Workstation

An open-source digital forensics toolset with pre-configured software for analysis.

More information:

SANS SIFT Documentation →

ThreatResponse GitHub Repository

A collection of tools to automate incident response and forensic investigations.

More information:

ThreatResponse GitHub Repository →

OSQuery

A tool for querying and monitoring endpoints, valuable for gathering real-time system information.

More information:

OSQuery Documentation →

Step-by-step guides

Setting Up AWS Security Services

AWS offers step-by-step tutorials for configuring services like GuardDuty, Security Hub, and CloudTrail.

More information:

AWS Documentation Hub →

Forensic Analysis with SIFT

A cheat sheet for using SIFT.

More information:

SANS Website →

Incident Response Playbooks

Tools like AWS Systems Manager allow you to automate response playbooks.

More information:

AWS Well-Architected Labs →

Conclusion and recommendations

Effective incident response in AWS requires preparation, adaptability, and a commitment to continuous improvement. The dynamic nature of cloud environments and the ever-evolving threat landscape demand proactive measures to protect resources and data. Below are the key takeaways and recommendations:

Key takeaways

Preparation is essential

Develop comprehensive incident response plans, enable robust logging and monitoring configurations, and train teams to manage AWS-specific threats.

Automation drives efficiency

Leverage AWS-native tools and third-party integrations to automate evidence collection, analysis, and remediation.

Forensic readiness matters

Ensure teams are equipped to collect, preserve, and analyze evidence from AWS services to understand and mitigate incidents.

Post-incident learning

Conduct thorough reviews after each incident to identify gaps, refine processes, and enhance the organization's security posture.

Recommendations

1

Adopt a layered defense strategy

Implement multiple layers of security, including network segmentation, IAM policies, and data encryption, to reduce the attack surface.

2

Invest in continuous training

Regularly train teams on AWS security best practices, new tools, and threat trends to maintain readiness.

3

Leverage managed services

Use managed security services like AWS Security Hub and Amazon Detective to enhance visibility and streamline response efforts.

4

Conduct regular simulations

Perform regular incident response simulations and tabletop exercises to test and refine response strategies.

5

Centralize monitoring

Use tools like CloudTrail, Security Hub, and GuardDuty to achieve unified visibility across AWS environments and ensure timely detection of incidents.

6

Establish automated workflows

Implement EventBridge, Lambda, and SOAR platforms to automate detection, response, and remediation workflows.

7

Evaluate and improve continuously

Use post-incident reviews to assess response effectiveness, update policies, and address any skill or tool gaps.

8

Prioritize compliance

Stay informed about regulatory requirements for data protection and reporting, ensuring all incident handling aligns with compliance standards.

9

Engage expert resources

When internal expertise is limited, consider partnering with cloud security experts or managed security service providers to bolster response capabilities.

/ CLOUD

How Darktrace can help

Darktrace delivers a proactive approach to cyber resilience in a single cybersecurity platform, including cloud coverage.

Darktrace / CLOUD is a real time Cloud Detection and Response (CDR) solution built with advanced AI to make cloud security accessible to all security teams and Security Operations Centers (SOCs). By using multiple machine learning techniques, Darktrace brings unprecedented visibility, threat detection, investigation, and incident response to hybrid and multi-cloud environments.

Darktrace's cloud offerings have been bolstered with the acquisition of Cado Security Ltd., which enables security teams to gain immediate access to forensic-level data in multi-cloud, container, serverless, SaaS, and on-premises environments.

Learn more about Darktrace / CLOUD for AWS:

Read the data sheet →

Dive into how Darktrace / CLOUD works:

Read the solution brief →

See Darktrace in action with a personalized meeting:

Request a demo →

■ About Darktrace

Darktrace is a global leader in AI for cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com