Playbook

# How MSSPs Can Add Incident Response Capabilities with Cado

CADO

# How MSSPs can Expand Their Incident Response Capabilities with Cado

As cyber threats continue to evolve in sophistication and scale, many organizations are turning to Managed Security Service Providers (MSSPs) to bolster their defenses and incident response capabilities. For MSSPs looking to expand their service offerings and provide more value to clients, adding incident response powered by a leading cloud forensics platform like Cado presents a compelling opportunity. Below, we explore the key reasons why MSSPs are partnering with Cado to offer comprehensive incident response services.

## The Growing Need for Incident Response

In today's threat landscape, it's no longer a question of if an organization will face a cyber incident, but when. With attacks becoming more frequent and damaging, having a robust incident response capability is critical for organizations of all sizes.

However, many companies lack the in-house expertise and resources to effectively respond to incidents, especially those involving cloud environments. This is where MSSPs can step in to fill a crucial gap. By offering incident response as a service, MSSPs can help clients:

- Rapidly investigate and contain threats
- Improve overall security posture and resilience
- Meet regulatory and compliance requirements
- Minimize damage and reduce breach costs

For MSSPs, adding incident response capabilities opens up new revenue streams while cementing their position as a trusted security partner. But to deliver these services effectively, MSSPs need the right tools - and that's where Cado comes in.

## How Cado Can Help

**"We use Cado Security for many investigations. Cado not only speeds up the process of acquisition and analysis, but it helps us by having more information to dig through and go deeper into the investigation." Matteo Brunati, CEO of Agorà Security**

**Ready to hear more about how Cado can help provide Incident Response? Try the Cado platform free trial.**

## The Cado Advantage for MSSPs

Cado offers the first cloud-native forensics and incident response platform, purpose-built to help security teams respond at cloud speed. Here are some of the key benefits Cado provides for MSSPs:

### 1. Rapid Deployment and Time-to-Value

With Cado, MSSPs can get up and running quickly to serve clients. The platform deploys via CloudFormation template or Terraform script in minutes. This allows MSSPs to rapidly onboard new clients and begin offering incident response services with minimal setup time.

### 2. Multi-Cloud and Hybrid Environment Support

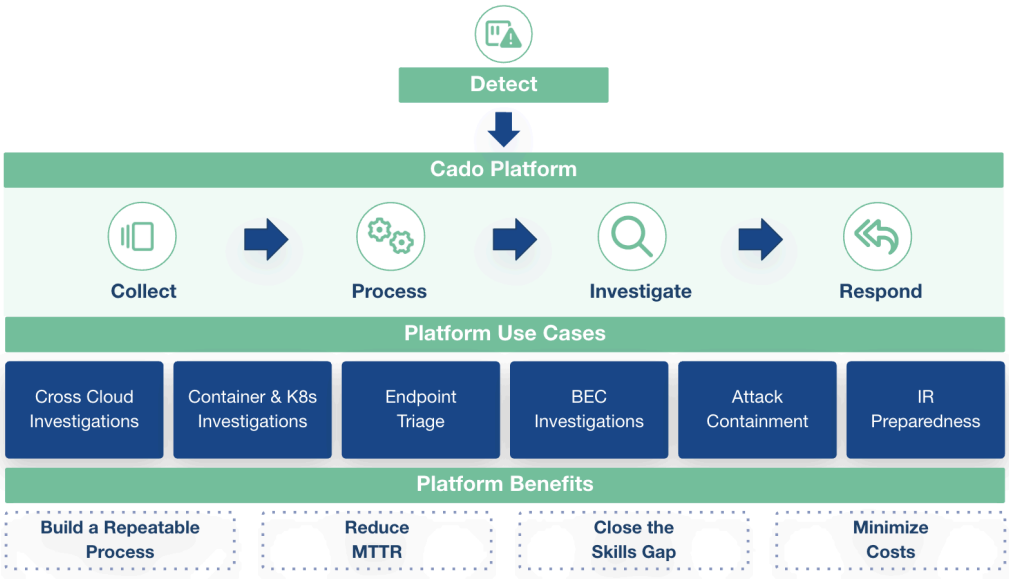
As more organizations adopt multi-cloud and hybrid architectures, incident response becomes increasingly complex. Cado enables investigations across AWS, Azure, GCP, as well as on-premises systems - all from a single pane of glass. This comprehensive coverage allows MSSPs to support clients regardless of their environment.

### 3. Automated End-to-End Workflow

Cado's automation capabilities are a game-changer for MSSPs. The platform automates the entire incident response process, from data capture to processing and analysis. By leveraging automation, MSSPs can:

- Reduce manual effort and increase efficiency
- Handle more cases with existing staff
- Improve consistency and reduce human error
- Decrease mean time to respond (MTTR)

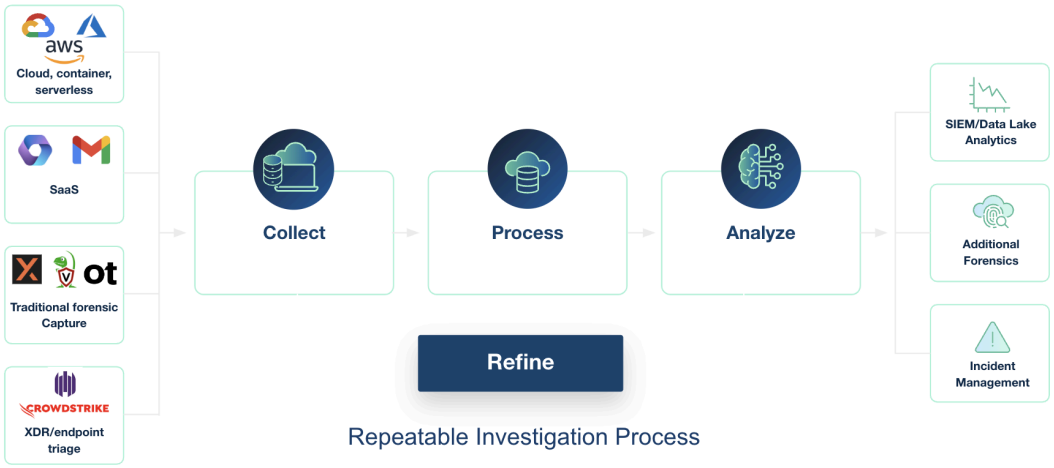
The Cado platform enables you to prepare for, respond to, and remediate incidents:




### 4. Forensic-Level Data Collection

Cado collects forensic-quality data across cloud workloads, containers, and even serverless functions - with no agents required. This deep visibility allows MSSPs to conduct thorough investigations and provide clients with comprehensive answers.

The Cado platform does this through enabling a repeatable investigation process during incidents, combining forensic data from multiple sources:




Repeatable Investigation Process

### 5. Cloud-Scale Processing

Cado's cloud-native architecture enables rapid, parallel processing of massive datasets. This allows MSSPs to quickly analyze large volumes of data from multiple sources, dramatically reducing investigation timelines.

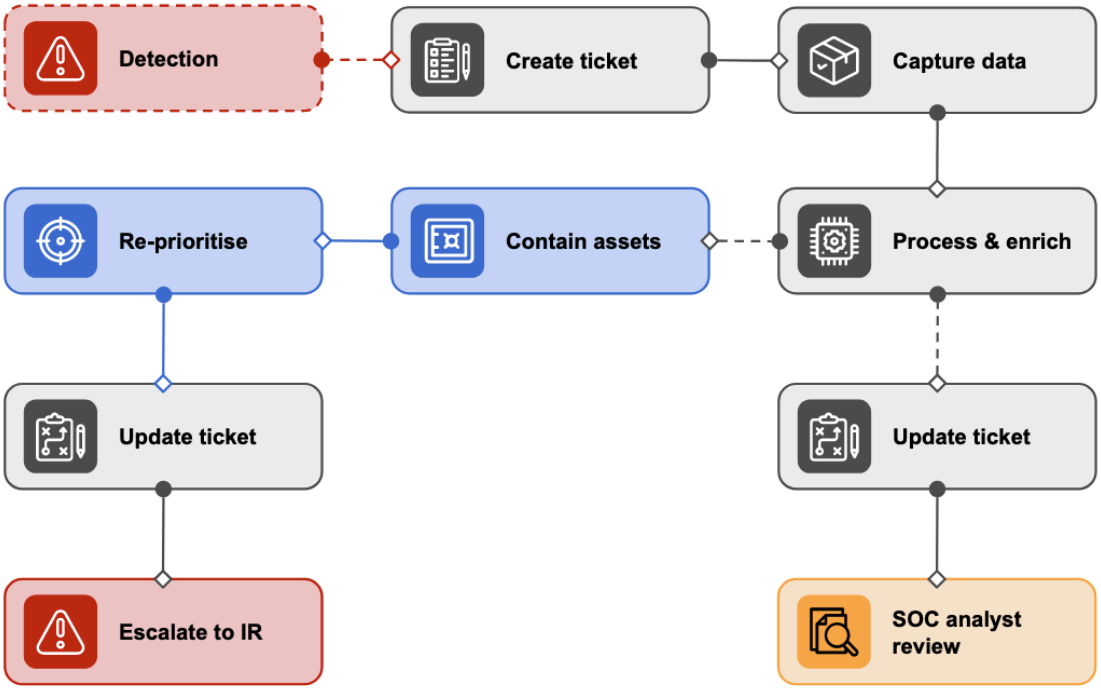
### 6. Advanced Analytics and Insights

The platform automatically surfaces the root cause, scope, and timeline of incidents. Built-in machine learning, threat intelligence, and YARA rules enhance investigations. These capabilities empower MSSP analysts to rapidly understand and respond to threats.

### 7. Integration with Existing Tools

Cado integrates seamlessly with EDR, XDR, SIEM, and other security solutions. This allows MSSPs to enhance their existing tech stack and processes rather than replacing them.

A typical workflow involves a detection from an XDR product (such as SentinelOne, Crowdstrike, Microsoft Defender etc.) or a Cloud Security product (such as GuardDuty, Wiz, etc), followed by automated investigation and resolution, logged in a ticketing platform:




### 8. Flexible Deployment Options

The Cado platform and all collected data can reside in the client's cloud environment. This gives MSSPs the flexibility to meet varying client requirements around data privacy and residency.

## Expanding Your Service Portfolio

By leveraging Cado, MSSPs can offer a range of high-value incident response services, including:

- Proactive threat hunting
- Incident investigation and forensics
- Breach containment and eradication
- Root cause analysis
- Compliance and regulatory support
- Reduce manual effort and increase efficiency
- Post-incident reporting and recommendations

These services not only generate new revenue streams but also position the MSSP as a strategic security partner rather than just a technology provider.

## Delivering ROI for Clients

When pitching incident response services powered by Cado, MSSPs can highlight several key areas of ROI for clients:

- **Faster Incident Resolution:** Cado's automation and analytics reduce MTTR by up to 80%, minimizing breach impact and costs.
- **Improved Threat Visibility:** Gain comprehensive visibility across cloud and on-premises environments to uncover hidden threats.
- **Reduced Reliance on External IR Firms:** Build internal IR capabilities to handle more incidents in-house, rather than handing off to third-parties.
- **Enhanced Compliance:** Maintain detailed forensic evidence to support regulatory and legal requirements.
- **Operational Efficiency:** Automate manual IR tasks to free up internal security teams for strategic initiatives.

# Getting Started with Cado

For MSSPs looking to expand into incident response, Cado offers a partner program to help you get started. Benefits include:

- Discounted pricing for initial deployment
- Technical training
- Sales and marketing support

By partnering with Cado, MSSPs can quickly build out their incident response capabilities and start delivering value to clients.

## Conclusion

As cyber threats continue to evolve, incident response has become a critical capability that many organizations desperately need but lack the resources to build internally. This presents a significant opportunity for MSSPs to expand their service offerings and deepen client relationships.

By leveraging Cado's cloud-native forensics and incident response platform, MSSPs can rapidly build out robust IR capabilities to serve clients across diverse environments. The platform's automation, scalability, and advanced analytics empower MSSPs to deliver faster, more comprehensive incident response - driving clear ROI for clients while opening new revenue streams.

For MSSPs looking to differentiate their offerings and become a true security partner to clients, adding incident response powered by Cado is a strategic move worth considering. The threat landscape isn't getting any simpler - make sure you're equipped to help clients navigate it.

If you'd like to hear more about partnering with Cado, please reach out.

### Ready to hear more about how Cado can help you be prepared for beaches?

Start Your Free Trial