Cloud security breach readiness

Four ways CISOs can prepare for cloud security incidents

kpmg.com

The sprint to the cloud has drastically changed how CISOs should view their security boundaries and requires a paradigm shift. While the cloud has offered unprecedented opportunity for resilience, scale, and innovation, security monitoring and incident response (IR) have not kept pace with the rapid change. As we think about how to solve for this dilemma, we should consider the following problem statement—how does an organization enable security monitoring and IR in the cloud and do it the "cloud way"?

Four ways to help prepare for cloud security incidents

1

Automate security monitoring and IR of cloud assets using cloud- native SOAR (Security Orchestration, Automation, and Response)

SOAR is everywhere today. One internet search and you will find no shortage of potential solutions ready to provide the next best orchestration platform. However, when implemented, too often SOAR development never reaches its potential. Security automation playbooks should do more than save minutes of tedious lookups and perform rudimentary tasks—playbooks should automate security investigations. When it comes to responding to incidents with cloud-native resources, cloud-native automation unlocks the ability to greatly increase the sophistication of automated response, speed up the time to response, and avoid challenges and inefficiencies associated with context switching between various cloud environments.

2

Set up and prepare your cloud digital forensics and IR environment before you need it

It's commonplace during security incidents to analyze threats using endpoint and forensic tools. However, traditional tools and capabilities are often only deployed to on-premise secure enclaves. Additionally, certain cloud-native resources may require analysis of available log data rather than a forensic analysis of the resource itself due to the nature of infrastructure-as-a-service (IAAS). During a cloud security incident, downloading compute resources locally for analysis will only drastically hamper the speed and effectiveness of analysis efforts. Instead of traditional log sources that might be found on disk, responders need to be prepared to extract data from cloud provider API endpoints and data stores in order to investigate incidents. Unfamiliarity with the extraction and interpretation of these log sources can become an enormous challenge in the midst of a fast-paced IR investigation. Being cloud ready also means having an IR environment in the cloud ready to go with all of the analysis resources, data collection scripts, licenses, and access rights to complete an entire investigation without bringing unprocessed evidence locally.

3

Retool your analysis, containment, and isolation capabilities to support cloud-native resources

The effectiveness of investigations hinges on being able to quickly identify threats, contain bad activity, isolate affected resources, and find root causes. Because Platform as a service (PaaS) and IaaS environment forensic data is recorded, collected, and stored differently than traditional on-premise environments, the capabilities needed by the IR team to perform critical tasks are likewise also different. In some cases, a cloud provider may not provide a sufficient built-in logging mechanism or retention period. This creates the need to develop and tailor new, often novel techniques to preserve audit log information, audit user activity, interpret identities, isolate machines, and audit file/storage access.

4

Rehearse your security response capability with cloud-focused adversary simulations

Security monitoring and IR teams need opportunities to test their preparations under adversarial circumstances. Adversary simulations that mimic real attacks offer a dress rehearsal for technical teams and a chance for management to refine its processes and plans. Given that many IR teams may have had limited experience responding to security events with cloud resources, adversary simulations provide the network defenders the opportunity to familiarize themselves with cloud evidence extraction, processing, and interpretation.

How can KPMG help?

KPMG transforms traditional methods of security monitoring and IR and brings these workloads to the cloud. Suitable for any phase of an organization's cloud journey, our cloud incident response capability enables the CISO organization to seize the capabilities of cloud offerings to monitor, detect, and respond to constantly evolving threats.

Our cloud incident response capability is based on our market-leading experience in security monitoring and IR. It gives security teams the capabilities they need to respond to cloud incidents while shifting focus and costs from operational monitoring to high-value tasks such as orchestration and automation.

Capabilities that KPMG brings to your organization include:

- An enterprise-ready operating model for cloud security monitoring and IR
- Cloud-native security IR automation playbooks powered by SOAR
- Security response playbook integration into the full stack of available security technologies, enabling automated remediation and response
- Cloud digital forensics and IR model labs for investigating incidents, including in federated models where security controls are distributed across cloud environments
- Advanced IR investigation orchestrations including evidence collection/preparation, resource isolation, and network containment for both Microsoft Azure and Amazon Web Services
- Ready-to-execute live adversary simulations and tabletop exercises for impactful cloud security events
- Automated digital forensics artifact triage and analysis through our KPMG Digital Responder analysis service.

Contact us

Ed Goings
Principal, Cyber Security Services
T: 312-665-2551
E: egoings@kpmg.com

David Nides
Principal, Cyber Security Services
T: 312-665-3760
E: dnides@kpmg.com

David Cowen
Managing Director, Cyber Security Services
T: 214-840-6489
E: dcowen@kpmg.com

Jordan Barth
Director, Cyber Response Cyber Security Services
T: 202-533-3989
E: jbarth@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.