Cloud Incident Readiness

It is estimated that in 2020 83% of the enterprise [1] workload will be in the cloud and for 66% of IT professionals securing the cloud is the biggest concern. However, we believe it is an opportunity for organizations to do cybersecurity 'right' from the start.
To do cybersecurity in the cloud the 'right' way it is critical that your procedures and technology are up-to-date and reflect the environment. We've spent years working cybersecurity incidents and we've noticed that threat actors adapt to the environment of their target, meaning that with the organization the threat actors are also shifting their focus and capabilities to cloud environments.

One of the greatest benefits of the cloud is the ease of deploying and configuring machines. The flexibility and ease of use introduces a new risk, which can be limited visibility and control over your environment. It is difficult for an organization to keep track of all the new instances and making sure detection and response capabilities cover the whole environment.

Therefore, it is important to evaluate the current capabilities of handling incidents and determine how they translate to your cloud environment. The following are several questions we use to evaluate cloud readiness for your organization:

- Is there documentation available that covers incident handling procedures for cloud environments?
- Is there a capability to forensically acquire logging, memory and disks from cloud environments?
- Is there visibility across all cloud assets and who has access to these assets?
- Are detection measures covering assets in cloud environments?

Ideally, your organization is able to answer all of the above questions, in order to be ready for incidents in the cloud. In our experience, organizations struggle to answer at least some of these questions and challenges, which is why we have developed our Cloud Incident Readiness (CIR) service. The aim of the service is to help organizations transform traditional incident handling procedures and technologies to cloud environments. Our team of incident response specialists continues to build cloud response capabilities using innovative technologies and best practices.

pwc

[1] "83% of Enterprise workloads will be in the cloud by 2020", Forbes, 2018

Please reach out to our experts for more information

Gerwin Naber
Partner
Cyber, Forensics & Privacy
Expertise:
Forensic Expert
T: +31 (0)88 792 63 02
E: gerwin.naber@pwc.com

Tom Driehuys
Director
Cyber, Forensics & Privacy
Expertise:
Incident Response
T: +31 (0)88 792 18 33
E: tom.driehuys@pwc.com

Korstiaan Stam
Manager
Cyber, Forensics & Privacy
Expertise:
Incident Detection & Response
T: +31 (0)88 792 72 60
E: korstiaan.stam@pwc.com

Additionally, we have developed proprietary technology that is not commercially available from anywhere to achieve some of the following tasks:

1. Automated memory acquisition of Windows and Linux systems for all major cloud providers;
2. Incident handling procedures covering acquisition, processing and analysis for all major cloud providers; and
3. Security monitoring guidelines and best practices to detect threats in cloud environments.

For this service, we follow industry standards on incident handling as described in the Computer Security Incident Handling Guide[2]. The CIR services focusses on the first two steps of the incident handling guide, Preparation and Detection & Analysis. We see that the biggest challenge for organizations is to adapt their current way of working and technology to cover cloud environments.

The service is tailored towards your requirements and organization because cloud environments differ. The service consists of the following phases and activities:

We will work with you and your team to get a better understanding of your environment and asses what materials are already available for incident handling in the cloud. Additionally, an analysis of the current configuration and procedures is done to get a better understanding of the current state of incident handling. The result of this phase is an analysis on the current state of readiness for incident handling in the cloud and an update to your incident handling documentation to cover cloud environments.

Using the results of the preparation phase, we can start with the implementation and integration of our technology to help you with acquisition of evidence. We will also document the required procedures for you and your team to acquire evidence in your cloud environment. Finally, an introduction to the available logging in the cloud is given for you to understand how this information can be used for incident detection and response.

In the processing phase, we will provide you with advice on how to best process the acquired evidence whether it is memory snapshots or logging of your cloud environment. The advice is tailored to your investigative environment to make sure it connects with your technology and way of working.

In the final phase, we aim to make sure all output from the previous phases leads to the desired results, which is being ready for when an incident occurs in your cloud environment. To this goal we make sure that your team understands how to analyze the evidence from your cloud environment. In practice, this means providing the team with help on what to search for in cloud environment logs or tips on analysis of hard disk snapshots and memory.

Why your company should prepare for an incident in the cloud?
Having the right preparation in place will significantly reduce the damage of a cyber incident financially, commercially and legally. Regulations such as GDPR require organisations to respond within 72 hours or face significant fines.

The Team
Our team consists of leading experts in the field of Incident Response and Threat Intelligence.
We have also developed a range of tools allowing us to acquire and process evidence from cloud environments. Some of our tools and knowledge have been open-sourced on our GitHub page.
We have been recognized as experts in the field by SANS who invited several of our team members to speak on the topic on Incident Response and Threat Intelligence topics at SANS conferences.

pwc

[2] Computer Security Incident Handling Guide, NIST 800-61 revision 2