IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with James Campbell

Carol Baker

As Cado Security's latest research reveals nearly 90% of organizations are suffering damage before security incidents in the cloud can be contained, we talk to James Campbell, CEO and Co-Founder at Cado Security about the challenges facing organizations and the critical role of incident response.

With *over 15 years experience helping global organizations tackle sophisticated cyber espionage and criminal campaigns,* ***James Campbell*** *is the CEO and Co-Founder of Cado Security (https://www.cadosecurity.com), and has a deep passion for cyber incident response, forensics and cyber crisis.*

Prior to founding Cado Security, James served as a Director at PwC building the Cyber Incident Response service. James' background also includes a career in intelligence, previously leading Australia's National Incident Response capability as the Assistant Director of Operations at the Australian Signals Directorate.

James is an active thought leader having spoken at various conferences, including Black Hat, cloudsec, CRESTCon, and the Forensics Europe Expo.

Tell our readers a little about yourself

I have been involved in digital forensics for over 17 years. First, at the Australian Signals Directorate in Australia, which is like the GCHQ or equivalent of the National Cyber Security Centre, where I was the System Director of Operations for seven years. I was fighting the bad guys in cyberspace before 'cyber' was really coined as the term. Whilst at the Australian Signals Directorate, I assisted with some of the IT security work with the London Olympics, creating some great connections before moving to London, where I worked with the cyber answer response service for PwC UK. I was part of a team there primarily responding to things like cybercrime nation state intrusions, and ransomware disruptive style attacks across customers in Europe.

I am now the CEO and Co-founder of Cado Security – although we are a UK headquartered startup, we operate globally, and have people across the UK and Europe, as well as the USA and Australia. That's quite a global footprint for a four-year-old company.

What has been the driving point in establishing Cado Security?

Before Chris Doman and myself set up Cado Security, as security practitioners in our various roles we would see organizations starting to embrace cloud technologies and shifting to the cloud. But when they wanted to investigate something suspicious happening in their cloud environment, not only was it very hard to do, but also the findings they were receiving were very hard to understand owing to the various technologies which make up the complex nature of cloud environments.

One of our customers likened their AWS environment to that of the 'Wild West' simply because they had hundreds of accounts and systems going up and down all over the place, and so just finding where that data is coming from, getting access to it, and then trying to bring that data into something which is usable and can be investigated before the data got recycled, took far too long and needed a great deal of effort. By the time they had engaged with the data, it was gone, and they were in an even worse position. Especially where a firm is heavily regulated or has compliance obligations, it finds itself in a worse position because an audit detection of the system will show that something has happened with sensitive data, but they have no way of telling anybody what happened. A scary situation for any business to be in. Compared to traditional on-premise systems, the cloud brings with it a great deal of risk because data is being recycled across the cloud infrastructure all the time, so analyzing that data takes a great deal of manual lifting, and a great skill set.

For instance, a Security Operations Centre (SOC) analyst has got 30 seconds to make a decision based on their detection – and that is not a lot of time when there is suspicious data volume coming from the system, and they are making a decision on behalf of an organization from a risk perspective. In many cases, the manual lift to go and investigate and escalate the findings is so high that most things just get closed, and just don't get investigated. If they do decide to investigate, organizations were finding that it was taking them up to two weeks to work out where that data is, how to get access to it, and then finally get it into something where they can get some level of context. That's just crazy – it's just far too long.

A SOC analyst shouldn't need to triage and get more information for that system – they should be able to do it at the click of a button. They shouldn't need to think about whether suspicious activity is coming from a laptop in Japan that has two virtual machines running in AWS; or whether it's a container system running in their infrastructure in Sydney, Australia, in account number 5622 of the customer. A SOC analyst needs to have the ability to ensure that at a click of a button, they can get more context and investigate the system. Chris and I realized that if we could automate the investigation and forensic process, we would really be on to something – and so Cado Security was born.

There have been many conversations among the security community about whether cloud forensics is just log analysis. Can you explain what is meant by true cloud forensics?

Gartner's research around Cloud Investigation and Response Automation (CIRA) found it to be quite a manual effort that resulted in limited context and disappearing data, so the term 'cloud forensics' began to emerge as a category in its own right. Cloud is bringing new challenges to the table from that perspective, and particularly with things like ephemeral infrastructure and short-lived infrastructure where systems are going up and down all the time. For example, many companies which heavily use containers and AWS will only have a 15-minute lifecycle. No company is manually going to be able to investigate suspicious activity – even if they have the capability to do so in the first place – in a container which only lasts 15 minutes after detection. So, you are left with an impossible task, of never being able to answer the question of ‘What happened, and what was the risk?’

Gartner recognized here that the keyword is ‘automation’ – the only way you can really get across how cloud works and the different ways in which we operate in technology today and infrastructure for their short-lived services is through automation. So, the race is on to go and grab the information needed before that system shuts down and the data gets recycled and lost forever.

Cado works across all industry sectors, regardless of the platform and infrastructure being used, with all data being fed into a central point at the click of a button. When detection happens, it automatically triggers Cado to go and grab the data before the container disappears. It identifies what has happened, what the risk impact is, and helps the analyst to resolve the problem so that it doesn’t happen again, or even just to confirm it is a false positive.

Please tell our readers about some of the key findings from the Cado report ‘Organizations Require a New Approach to Handle Investigation and Response in the Cloud’.

Unsurprisingly, hackers are absolutely 100% still targeting cloud-based services. Why are they doing that? Because data is moving to the cloud, so naturally they are moving to the cloud as well. The complexity of the cloud means that there are misconfigurations all the time, and hackers are taking advantage of things not being set up correctly. We recently ran a demonstration at the RSA conference to show how often a system can be compromised. At the event we had just one exposed service, and delegates were able to watch how the vulnerable service was being compromised on average every 15 to 20 minutes.

The other thing we noticed in our research is that the lead time to respond and investigate incidents is quite high – typically around three to five days to investigate something in the cloud versus an on-premise environment. This means that a business can have an attacker running around its network for days stealing data. That’s crazy. A lot of people just don’t understand the cloud and there is still a great deal of education to do, and the skills shortages in the IT sector aren’t helping.

For example, I had a great conversation once with a big US insurer, and the security guy was so frank and honest, and a real advocate to the community. He said, “Look, James, I’ve been in security for 20 years. We’ve just shifted everything in AWS. I know how to get firewall logs out of my physical firewall in the data centre. I know how to rip a laptop hard drive out, you just go over and grab it and rip it out and then do some analysis on it. But I have no idea how Kubernetes works or lambda, or how I even connect to a container in AWS. Organizations expect their IT staff to know every single type of technology used in the cloud. I have system ‘x’ showing something suspicious, and I just want to look at system ‘x’. In all honesty, I don’t mind what technology it is, I just want to look at it right now because I need to be able to respond quickly, and reduce that mean time to respond from days to minutes.”

As data moves to the cloud, we see more complex attacks. We ran a demo that showed how an attacker can move from a single service that was compromising a container to the broader whole entire AWS estate. And they do so just by hopping through multiple systems through an initial exposed service, and because that container disappears, and no one investigates the initial detection, no one's any the wiser that the hacker has already moved on to the rest of your cloud estate and has administrative control. So pretty scary.

When it comes to cloud forensics, what does ‘Chain of Custody’ mean?

Chain of Custody is a kind of ediscovery in a digital forensics space, especially when it comes to any form of legal proceedings where you are required to show some level of accountability and auditability. Chain of Custody shows the data that you had used during your investigations to come to your conclusions, and provides evidence that the data was captured in the right way and hasn’t been manipulated or corrupted. It’s important that when someone independent of you follows the same steps, they come to the same conclusion with the same data source, and feel confident that it has maintained integrity throughout the process.

What are some of the challenges facing vendors when it comes to providing forensics solutions?

In many ways, technology is evolving faster than we can learn it, so it is important that both organizations and vendors upskill their entire workforce so that they become familiar with cloud technologies in all their different variations.

In our partnership with Wiz Integration (WIN) platform, for instance, we can bring the power of the Cado Security platform to the partner ecosystem so that Wiz customers can seamlessly integrate Cado into their existing cloud security workflows. This enables our mutual customers to rapidly kick-off forensics investigations of AWS EC2 instance, and automate forensic investigations of cloud resources, using Wiz’s one-click forensics capabilities to accelerate the path to root cause and remediation. Using Cado’s AI Investigator, customers receive deep forensics analysis capabilities to better understand the root cause, scope, and implications of cloud-based threats. Additionally, Cado gives customers instant access to cloud resources and potentially compromised systems without the need to configure additional access requirements or having to work through other teams, saving analysts critical time during an investigation. This all allows companies to streamline their security regardless of where they may be on their cloud journey.

Do you have a closing thought for our readers?

No organization should be afraid of learning about the cloud and the new risk it brings to the table. Cloud is very different to deal with compared with on-premise, bringing different challenges and new ways of doing things. A company can’t just lift and shift its approach to security from on-premise to the cloud and expect them to be the same. Cloud is very different. The flip side of that is the cloud does provide loads of opportunity with the technology itself. By using cloud native solutions, we can automate the end-to-end security lifecycle and give companies peace of mind when they embrace the cloud technologies in their organizations.