Hello, tomorrow.

Case Study: How a digital transformation helped a major real estate developer protect against cyber crimes

Real estate development
This successful family-operated real estate developer, based in Hong Kong and boasting operations in Greater China, has been in business for several decades. The company’s vision is to create shared value and tie its business success to social progress. Core business areas include investment in property and property development, as well as commercial aircraft leasing, construction, insurance, hotels and other strategic businesses.

Challenge: Lessons learned the hard way
The developer noticed the market shift toward technology companies and innovation. With the government encouragement for developing technologies, the market was becoming more competitive than ever. The real estate developer understood that in order to preserve business and promote growth, going digital was crucial. But it wasn’t until suffering through a ransomware attack that the company began to make changes.

The company believed that the attack was in part due to a lack of employee awareness, as well as the growing work-from-home arrangements which provided a larger attack landscape from remote connection gateways. The real estate developer began looking for a managed security service to:
• Uplift and continuously monitor its environment.
• Avoid another major cyberattack incident.
• Secure its digital transformation journey.
• Move to 100% cloud native.
• Provide threat intelligence and behavior analysis.

Solution: The PwC Playbook
It was important that the real estate developer’s digital transformation make the leap into the cloud and it chose PwC’s managed security services to integrate AWS in cloud native. The PwC 24x7 security operations center in Hong Kong has served over 50 clients with cloud workloads. It is a well-established cybersecurity and cloud consulting firm in the region with prominent experience with ransomware attacks, and it maintains a strong partnership with AWS.

AWS in cloud native provides a mature solution for investigation and forensics with CloudTrail and GuardDuty, as well as stability, scalability, and flexibility for PwC consultants to architect the solution according to needs. AWS in cloud native can also respond automatically, performing reliably against cyberattacks at any time and on any scale.

Throughout the years, PwC has obtained threat intelligence and data points on hacker behavior within AWS environments. PwC has developed an incident response playbook with more than 50 correlation rules, leveraging metrics collected from CloudTrail, CloudWatch, Security Hub, and GuardDuty. These metrics are mapped against the MITRE ATT&CK matrix for full visibility throughout the cyberattack kill chain.
Solution: The PwC Playbook (Continued)
But the AWS platform is only the first entry point of the attack chain and it’s impossible to see and manage everything at the AWS platform level. Oversight at both platform and host levels is crucial to detecting and preventing more targeted attacks such as ransomware through spear-phishing attacks.
After integrating the real estate developer’s AWS environment to the PwC 24x7 security operations center, PwC deployed a 3rd party endpoint detection and response solution, providing visibility on the cloud platform level, as well as the ability to correlate events at the endpoint and host level. PwC then developed custom rules to correlate AWS events from CloudTrail and GuardDuty with the endpoint detection and response alerts, providing a holistic view throughout the cyber attack kill chain.

Results: Cracking down on cyber crimes
The real estate developer defined key performance indicators and risk metrics for monitoring the new solution and security service, such as incident response time, patching timeliness, virtual machine hardening coverage, etc. With AWS in cloud native and PwC’s managed security service, 100% of these indicators and metrics have been met. Other results include:
• 100% coverage in client’s server side and endpoint environment
• 100% full correlation between AWS metrics and the endpoint detection and response solution
• 100% cyber operations service-level agreement compliance
• Complete transformation into the cloud
• A holistic view to correlate AWS events with client’s server side and endpoint activities

About PwC
At PwC, our purpose is to build trust in society and solve important problems. PwC is a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services.