IDC EMEA, 389 Chiswick High Road, London, W4 4AE, U.K. Tel.+44.20.8987.7100 www.idc.com

IDC CUSTOMER SPOTLIGHT

HPArcSight ESM Solution Helps City University to Safely Increase Student Numbers by a Third While Going Mobile

July 2013

Sponsored by HP

Introduction

City University of Hong Kong is a public research university founded in 1984 as City Polytechnic of Hong Kong and became a fully accredited university in 1994.

City University offers more than 130 bachelor degree programs in six schools and colleges and a community college, covering a wide range of subjects from the arts to science and engineering.

There are approximately 34,000 students, with around 13,000 undergraduates in the university itself and 6,000 students in the community college.

The university has around 3,500 staff members, of which almost 1,000 are academic or teaching support. City University also supports over one hundred thousand alumni with access to services.

Since its inception City University has been at the forefront of technology adoption, implementing an ERP platform over a decade ago, and was among the first to use elearning management solutions.

Technology plays an integral part of both operations and education delivery at City University. CIO Dr Andy Chun describes the approach as "a unique discovery-enriched curriculum to encourage our students to innovate and make original discoveries, and to learn what it means to create new knowledge, communicate it, curate it, and cultivate it to benefit society. Technology plays a very important role in the discovery and learning process."

Snapshot

Organization: City University of Hong Kong

Operational Challenge: Handle a move to mobile services access and increase undergraduate numbers by a third while increasing service quality.

Solution: HP ArcSight Express

Project Duration: From concept to production, first implementation phase took six weeks.

Benefit: Investigations into suspicious activities dropped from weeks to hours, freeing up skilled resources to work on IT service delivery.

Challenges and Solution

City University was faced with two major challenges in delivering information technology services to students and staff across the organization.

The first was to adapt to the new ways in which students and staff are interacting with IT services. In 2010, almost all access used desktop or notebook PCs and there was almost no remote or mobile learning. In just two years this situation has completely reversed so that over 70% of students and staff now use mobile devices such as smartphones or tablets in addition to a PC to access services via mobile services or remotely. In the last year alone, over 130,000 individual wireless devices connected to City University's WiFi network.

In addition, City University has a large pool of loan notebooks that are made available to students to work on projects or deliverables if they don't have a PC or mobile device of their own to use.

The second challenge was a change in undergraduate degree courses from three years to four years. As there was no real change in the number of students enrolling per year, this resulted in the number of undergraduate students swelling by a third due to the extra year, all of whom need access to services.

The end result was a vast increase in the number of users and devices accessing services, which all needed to be secured and protected. Dr Chun realized that growth was challenging existing security operations, which were starting to be overwhelmed. He identified a number of areas that were particularly challenging:

- City University has a large number of security devices and tools in place to enforce security policies and protect users, but each has its own logging format and monitoring tools.

- Identifying anomalous behavior, such as malware infections, hacking attacks or security breaches, was proving to be unworkable due to the millions of log entries from multiple sources being returned, all of which would have to be analyzed to try to pinpoint attacks because there was no linkage or correlation between them.

- It was difficult to extract trend information from events and it was impossible to relate the events from the various infrastructure components into an application or business service oriented view. This made it difficult to report to senior management on what had occurred.

- Changes in the infrastructure meant laborious work to reconfigure the event collection connectors.

After analysis of the problem and advice from third parties, City University determined that a central monitoring system would be needed to get on top of the challenges. There was already a log management solution in place that had been developed to secure a number of UNIX servers in the datacenter, but this was proving to be difficult to adapt to the new requirements. It could not easily process logs from multiple sources, and could not deal with log files that have multiline entries. It would also frequently return false positives, which would divert limited resources from dealing with real issues.

City University therefore looked for dedicated security incident and event management (SIEM) solutions and invited two vendors to propose proof of concept (PoC) along with requirements and internal test cases that made up the success criteria. Within a week, HP ArcSight delivered a working PoC that satisfied the success criteria and in particular the multiline log event processing capability. Compared with the competition, HP ArcSight had very knowledgeable implementation and support engineers that formed a good relationship with City University, giving them the confidence to move forward into production.

Implementation

Once the PoC was successfully demonstrated and HP ArcSight Security Intelligence Platform was selected, sign-off was given to implement the solution. The plan involved the following steps:

- Deploying ArcSight Express
- Integrating logs from multiple sources including active directory services, routers, and security devices
- Generating reports of critical events
- Implementing a Service Monitoring Dashboard

Because the initial success criteria included many test cases that were daily operations processes for City University, the implementation ran smoothly overall and slightly ahead of plan.

There were some issues to resolve during the implementation around the integration of some devices and applications, such as firewalls and networking devices with particular configurations. The problems were identified and the solution took a few days of development to implement and the overall solution was in production within six weeks.

Benefits and Challenges

Once operational, the HP ArcSight Express started to provide immediate benefits. The most immediate and noticeable benefit was a marked reduction in manpower requirements, particularly around troubleshooting issues as they arose. In the past, this would involve mobilizing many teams of people to work through the various systems individually, but this now automated centrally. With City University facing budget and manpower freezes, this adds a lot of value by freeing up skilled people to work on other initiatives.

Turnaround times when investigating anomalies have also improved dramatically. Previously it would take up to a month to be able to gather all the logs together and then organize staff to analyze them. With HP ArcSight, this now takes hours to do as the system stores the logs and joins them together to allow automated correlation across multiple systems.

The platform also allows new rules to be easily introduced to catch future incidents in progress rather than detecting them afterwards and having to spend time and money remedying the problem.

Despite the success of the implementation, there is still more to be done. Budget, resources, and skills have meant that the existing implementation is not yet where City University needs to be. Two further implementation phases are planned to make more use of the capabilities of the platform. Phase two is already underway, and is a shorter term optimization project to build out log storage and develop management dashboards.

Phase three, planned for the next academic year, will involve upgrading the platform to HP ArcSight Enterprise Security Manager (ESM) and extending coverage even further into IT service delivery. This will include datacenter environment monitoring such as power, temperature, and humidity as well as end-to-end IT service monitoring and linking to the CMDB.

City University's SIEM solution is a unique approach that pushes the boundaries of the HP ArcSight capabilities. The result is an SLA dashboard that makes use of artificial intelligence (AI) techniques for intelligent threat correlation. This is used to create a "causal network" that defines relationships and hierarchies among various devices. The system is able to sort through and make sense of multiple logs and log entries to intelligently pinpoint attackers or source of problems; thus reducing human processing time during emergency situations.

Conclusion

The ability of HP ArcSight Express to gather log and event information across multiple sources and to handle the most complex information has enabled City University to gain invaluable insight into activities across the entire IT infrastructure while cutting the manpower required to do so. This has allowed IT service quality to improve even with a sharp increase in demand for access to services.

These improvements in security and service quality have helped towards City University receiving ISO/IEC 27001:2005 Information Security Management Systems Certification from the British Standards Institution in 2013; the first University in Hong Kong to do so. The University was also named a 2013 Computerworld Honors Laureate for its Sustainability Project that created a greener campus by providing a highly secured environment to archive university personnel and financial documents.

Methodology

The project and company information contained in this paper was obtained from multiple sources, including information supplied by HP and questions posed by IDC directly to City University of Hong Kong employees.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.
Global Headquarters:
5 Speen Street
Framingham, MA 01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com