PCCW Global provides organisations with a unique behavioural-based security

A new threat intelligence platform finally cuts through the noise of overwhelming numbers of security alerts, and enables organisations to be proactive in their fight against malicious cyber-actions

Yiannis Giokas, CEO, Crypteia Networks

Enterprises and consumers are ever more impacted by cyber-security issues as threats proliferate and risks increase. It's a problem that isn't going away, and operators have the opportunity to play a critical role because of their unique position as the carriers of large volumes of global internet traffic. That role enables operators to identify abnormal patterns and behaviours and provide customers with relevant alerts and mitigation strategies.

However, operators are yet to cement their position as providers of cyber-security services, and there is some lack of clarity as to how they will fit into an already crowded ecosystem of security providers and systems. There is a bewildering array of technologies and systems that organisations can use to combat fraud, and there is a risk that this can cause confusion or enable real security threats to be masked by the sheer volume of alerts.

MORE EFFECTIVE SECURITY INTELLIGENCE

Managing security alerts and events has traditionally been performed by security information and event management (SIEM) and log management systems, which consolidate all the data from the various security tools and brings the disparate data back to a central point. This centralisation is significant because data from firewall logs or intrusion detection logs, for example, viewed in isolation don't have meaning unless they are correlated to or triangulated with data from other systems.

However, SIEM tools address only the centralisation aspect and are still lacking intelligent functionality in terms of being able to identify what is happening and enabling users to be proactive. Organisations still need the capability to address an attack before it happens and the trend data and insights that exist can enable attacks to be foiled proactively.

CYBERGUARD THREAT MANAGEMENT SERVICE

This need for greater functionality and behavioural insight was the motivation for Crypteia Networks to develop its MOREAL — MOnitoring, REporting and ALerting — platform to provide useful data on a single screen to enable organisations to be proactive in combating security threats.

"The MOREAL concept dates back to 2011 when we were looking for a way to have a single pane of glass for all the environments Crypteia Networks was offering security services to," explains Yiannis Giokas, the chief executive of Crypteia Networks, which was acquired by PCCW Global in 2014.

"The solutions available at that point in the market were focused more on log collection and building custom rules to get alerts via SIEM and log management systems, but there was no ability to correlate that knowledge against knowledge that you had from other networks, other sources or the regular behaviour of any given asset."

The MOREAL platform is actually one of two components that make up the CyberGuard Threat Management Service, the flagship product in PCCW Global's CyberGuard family of security services. The second element of the service is supported by a security operations centre analyst. The SOC analysts work with clients in helping guide them in their security operations and, in some cases, actually manage some of the devices. Other CyberGuard security services from PCCW Global include managed and hosted firewall services, managed router services, and managed anti-DDoS — distributed denial of service — services.

EARLY WARNINGS

The need to manually correlate and make sense of all of this data was an oppressive burden and this led Crypteia Networks to start developing the MOREAL system. "We wanted to create a platform that would enable us to provide our clients with security in depth — not in width," says Giokas. "That means fully profiling each IP address and asset within the organisation and utilising our external knowledge and the intelligence we derive from other networks we monitor or incidents we handle so we can minimise the time to identify and respond to attacks."

Giokas describes MOREAL as a fully-fledged Threat Intelligence platform that, through behavioural analysis, machine learning and correlation across multiple networks enables early warnings for cyber-attacks, identification of misconfigurations on the security infrastructure and misuse of the network resources by users to be identified.

"Instead of bombarding security analysts with alerts about anomalies in user, network and system behaviours, we have a second layer of reporting in which we address all the known anomalies, misuses and any known threats," explains Giokas.

"We add in any reportable anomalies that have not yet been found by standard security tools to be threatening or malicious, and we present all of that clearly in a single screen. The user doesn't have to be an expensively trained security specialist to understand the issue. They can drill down into the individual alerts if they want to, but our interface avoids deluging them with alerts that are almost impossible to find the root cause of."

Being owned by PCCW Global has enabled Crypteia Networks to build the capability to monitor enterprise-class IP networks utilizing the MOREAL platform.

"Monitoring a network like PCCW Global's worldwide infrastructure network gives us visibility into threatening behaviours while they are still on the rise, so when a big command and control event happens, we can see the potential threat on the PCCW Global and other networks," he adds.

"This provides an early warning and is, therefore, very important and one of the values that PCCW Global derives from the acquisition of Crypteia Networks. We see nearly 15% of the global internet as it traverses the PCCW Global network, so we have a very large volume of traffic flowing through our infrastructure, and add to that the insights from customers who receive our service, whether or not they're connected to a PCCW Global network. This is how we have grown our knowledge of activities that are either acceptable or malicious."

BEHAVIOURAL ANALYTICS AND MACHINE LEARNING

For PCCW Global, this new cyber threat protection capability provides an additional option to its service provisioning capabilities. "It's the next evolution in service provisioning to our clients," says Bob Flinton, the senior executive of product marketing at PCCW Global's CyberSecurity Services Division.

"Most operators only provide at the highest levels a managed SIEM offering, and because of that, I think we're the only one providing a machine-learning, user analytical behaviour-based approach through our technology platform and our security operations centres," he says. "Having our global managed security service centres means we can provide a real-time response." For Giokas, providing that additional level of functionality above that which SIEM systems provide is compelling. "SIEM systems only provide a post-mortem view, but we're enabling clients to be proactive," he says. "This is why we provide a number of dashboards to enable them to see the attacks that are hitting the networks and the potential mitigation methods."

GLOBAL THREAT DATABASE

Flinton adds: "The coverage of the PCCW Global cloud means we're able to see activity that could be malicious in certain regions or sectors around the world and in various markets and warn other relevant clients," he adds. "That's a huge differentiator for PCCW Global."

Significantly, organisations don't have to be a PCCW Global network client to benefit from the threat intelligence service. It sits on top of any infrastructure and is non-intrusive, so expensive network agents and probes are not required on the network.

Giokas explains that the technical approach is innovative and currently has two patents pending at the US Patent and Trademarks Office. "The first patent is focused on identifying attack paths and providing mitigation suggestions by optimising intrusion detection and intrusion prevention systems," he says.

"The second patent is focused on crowd-sourcing threat intelligence via aggregating and storing knowledge that exists in various forms in a number of open source security intelligence sources," he adds. "This intelligence is derived by analysing incidents that have been handled by Crypteia's security operation centres, Twitter feeds, forums, the darknet and other sources in a completely unstructured format. The knowledge that is the outcome of cross-network event correlations, which enable us to have an encyclopaedia of threats, malicious behaviours and patterns which minimises the time taken to identify known and unknown threats."

ADDITIONAL LAYER OF DEFENCE

The Crypteia MOREAL platform is an additional layer of security that builds on the existing security organisations and network providers have in place. Complementary to SIEM and log management systems, its strength is in being able to bring all the disparate data together in a usable format on a single screen. That, coupled with the sheer volume of data insights it analyses, and the learning it accomplishes about malicious behaviour and threats, creates a further step towards achieving optimal security.

MOREAL has also garnered critical acclaim around the world, having recently won industry awards, including the World Communications Awards recognition for Best Innovation 2015, the Global Telecoms Business Innovation Award 2015, and the Enterprise Europe Network New Success Award 2014.

"We've invested a lot of time and effort to make something innovative that even in the long term will continue to be a differentiator," says Giokas.

www.pccwglobal.com
www.crypteianetworks.com