Lumen Newsroom

Multi-layered, single-platform service package provides digital businesses with key capabilities to monitor, analyze and protect their data

SINGAPORE, May 8, 2020 /**PRNewswire**/ -- **CenturyLink, Inc.** (NYSE: CTL) has launched its **Managed Security Behavioral Analytics (MSBA)** service package in Asia Pacific. This single-platform offering provides organizations with the capability to monitor for and detect insider threats on critical assets. It employs behavioral analytics algorithms to find malicious user activities and automates the review of privileged account activities. It also detects events that pose a risk, known attacker behavior, anomalous network activities and deviations in account behavior.

According to a new report from the Ponemon Institute called "2020 Cost of Insider Threats: Global," the average global cost of insider threats rose by 31% to $11.45 million, and the frequency of incidents spiked by 47% compared to 2018. The study also highlighted that negligent employees or contractors, who were found to have caused 62% of insider threats, created the highest financial burden of the profiles, costing an average of $4.58 million per year.

"Enterprises today face a stark new reality where cyberthreats go beyond ransomware, malware and perimeter data breaches," said Cathy Huang, associate research director for services and security at IDC Asia/Pacific. "Organizations are overlooking a potential threat vector from within their businesses, where the risk of sensitive data loss and breaches are high – their employees. These insider acts could be classified as unintentional or malicious, but they are equally impactful to a company's overall cyber defense efficacy and can possibly damage the reputation and trust a customer has given them."

"As more digital businesses move their vital infrastructure online, it is crucial that they have a proactive cybersecurity strategy to monitor and protect their assets," said Cheah Wai Kit, director, product management (Security), CenturyLink Asia Pacific. "Cyberthreats within the organization can possibly go unnoticed for months, or even years. The CenturyLink Managed Security Behavioral Analytics service delivers an integrated approach of unique technologies that are monitored and managed by the CenturyLink Security Operations Center. This solution offers business leaders advanced visibility into potential threats that may be hidden within their networks, IT infrastructure, applications and databases."

Many companies have detection controls on their network or can implement controls when an outsider (non-employee) tries to access their company data, and they can mitigate the threat with physical security controls. The threat that is harder to detect, however, and who could cause the most damage is the insider – the employee with legitimate access. Insiders might steal solely for personal gain, or they may be a "spy" who are stealing company information or products to benefit another company, organization or country.

With the MSBA service, organizations can:

- Detect and deter insider cybersecurity breaches by monitoring for deviation in account behavior, with a focus on security-relevant events posing a risk.
- Monitor for signs of credential theft, hijacked accounts, malicious account activities and login anomalies.
- Automate the review of privileged account activities to find unauthorized transactions and

malicious activities at the operating system, application, and database levels.
- Detect malicious server network traffic for signs of backdoors, lateral movement, malware traffic and data exfiltration.
- Detect signs of an early breach to minimize dwell time.

The MSBA service package features:

- Intelligent analytics: Automated threat-detection algorithm reviews both user and network activities to identify potential indicator of compromise (IOC) risks based on profiled user personas, known attacker behavior based on threat intelligence, and industry frameworks such as MITRE ATT&CK.
- Embedded detection: Lightweight sensor/agent runs on servers hosting critical assets, data and applications.
- Privileged account monitoring: Monitors security-relevant, privileged operations for anomalies and unusual operations such as abuse of data access, unauthorized transactions and excess privileges.
- Behavioral baseline: Gathers insights into individual user personas to establish a pattern of normal behavior from which to identify anomalies and provide quick detection of insider threat indicators.
- Real-time discovery: Provides 24/7 monitoring via integration into the **CenturyLink Security Operations Center (SOC)** for triage and escalation.
- Platform agnostic: Supports multiple operating systems.

CenturyLink cybersecurity experts will also be available to provide consultation as part of the MSBA service package. Their role is to provide advice and make recommendations to help organizations improve their security postures.

"The rising significance and impact of cybersecurity is no longer just technical or compliance issues, but also business and strategy concerns to which Asia Pacific organizations are paying closer attention," said Huang. "With Asia Pacific organizations experiencing stronger regulatory pressures and recognizing investment in security as part of their digital transformation battleplan, they are looking for service providers to support their business objectives. The value brought by Managed Security Services Providers (MSSPs) to the ecosystem is clear. To build effective cyber risk strategies, a MSSP must align cyber defense controls with business goals. This requires deep industry expertise and capability to develop industry-specific threat models that go beyond conventional infrastructure layer monitoring."

"What we are offering is peace of mind and a testament to our commitment as a trusted Managed Security Services Provider to our customers to **See More and Stop More**," concluded Cheah. Besides MSBA, CenturyLink's SOC is also responsible for delivering our portfolio of detection and mitigation services, including analysis and leveraging threat intelligence data provided by Black Lotus Labs, CenturyLink's threat research arm, which analyzes 190 billion NetFlow sessions and over 3.6 million security events every day.

Additional Resources:

- Learn more about CenturyLink's Managed Security Behavioral Analytics: **https://www.centurylink.com.sg/security/managed-security-behavioral-analytics.html**

- Request for a free security consultation: **https://www.centurylink.com.sg/resources/offer/free-it-security-consultation.html**

About CenturyLink

CenturyLink (NYSE: CTL) is a technology leader delivering hybrid networking, cloud connectivity, and security solutions to customers around the world. Through its extensive global fiber network, CenturyLink provides secure and reliable services to meet the growing digital demands of businesses and consumers. CenturyLink strives to be the trusted connection to the networked world and is focused on delivering technology that enhances the customer experience. Learn more at **https://news.centurylink.com/**.

Appendix

Customer Scenarios

Use case 1: December 30 2019 - CenturyLink's SOC detected suspicious security anomalies with a Privileged User Account's (PUA) activities its customer IT environment.

The first suspicious observation was when the PUA logged into one of the customer's ERP server. He was last seen logging into this server 69 days ago. Analytics shows his login activities through the Domain Controller was 83 times higher than usual.

He was accessing multiple servers which he has never logged into before. There were 19 different source IP addresses used by this PUA to access the network.

While there were unusual login activities, CenturyLink SOC analysts performed an in-depth investigation which revealed that no data was exfiltrated nor were there other suspicious signs of malicious activities. The case was escalated to the customer and CenturyLink learned that this PUA was carrying out an impromptu, and urgent maintenance window.

Use case 2: Mid August 2019 - CenturyLink's SOC detected possible security events when there were suspicious DNS requests being sent through the customer's Domain Controller. This resembles Domain Generation Algorithm (DGA) patterns, which are seen in various families of malware and generates a large number of domain names that can be used as rendezvous points with their C2 (Command & Control) hosts.

Upon this discovery, CenturyLink SOC analysts took immediate threat-hunting action. Further investigations found that the endpoint device's IP which generated the DNS traffic patterns were connected through the customer's BYOD guest network. The DNS destination host was also found to be categorized as malicious or suspicious. Sometimes, DNS tunneling can be used as a way to camouflage C2 communications.

The incident was escalated to the customer to determine if the endpoint device is one of their corporate assets or if it belongs to a visitor.

Photo - **https://mma.prnewswire.com/media/1165561/Managed_Security_Behavioral_Analytics.jpg**

Logo - **https://mma.prnewswire.com/media/628320/CENTURYLINK_Logo.jpg**

For further information: Media Contacts: CenturyLink , Darryn Lim, 67688085,

darryn.lim@centurylink.com; Ying Communications (a FINN Partners company), Danial Cheah | Syafiq Rahman, 67795514, centurylinkprasia@finnpartners.com

---

Additional assets available online: (2)

https://news.lumen.com/2020-05-07-CenturyLink-Offers-360-Degree-Cyber-Defense-Analytics-Service-to-Enterprises-in-Asia-Pacific