ENTERPRISE
SECURITY

WWW.ENTERPRISESECURITYMAG.COM
JULY - 22 - 2019

Top 10 SIEM Consulting/Services Companies - 2019

With an ever-increasing number of enterprises and the corresponding rise in data and edge computing devices, the global cybersecurity industry is forecast to see an 8.7 per cent rise in the current year. This upsurge in the cybersecurity market makes it an uphill task to keep pace with the rising malware attacks and cybercrimes globally. In such a scenario, security information and event management (SIEM) plays a pivotal role in advanced threat detection and monitoring. They can analyze the threats, deliver insights and provide the response necessary to combat the cause.

In tandem with the technological evolution, modern SIEM service providers have become a necessity in the delivery of complex strategies that can implement these technologies. Along with threat management and general monitoring in SIEM, targeted attack detection is likely to be a major component in the coming days. SIEM consultants need to be able to combine on-premises and cloud deployments to create a cloud-based SIEM solution that scales and secures user journey to the cloud, providing deep insight into the security ecosystem and applications. The challenge with leveraging massive amounts of information is that it comes in an array of unpredictable formats, but with the advanced SIEM, it is possible to obtain real-time insights into this high volume of data, with a greater capacity to extract, store and analyze.

To help business providers in selecting promising SIEM service providers, a distinguished panel of prominent marketing specialists and analysts, along with Enterprise Security Magazine's editorial board has assessed and shortlisted the start-up companies offering pioneering technology services in the SIEM industry. This listing gives a comprehensive understanding of services that can be implemented to optimize your business process.

We present to you our "Top 10 SIEM Consulting/Services Companies - 2019."

Vertek

recognized by ENTERPRISE SECURITY *magazine as*

TOP 10
SIEM
CONSULTING/SERVICES COMPANIES - 2019

An annual listing of 10 companies that are at the forefront of providing SIEM consulting services and impacting the marketplace

Company:
Vertek

Description:
Founded in 1988, Vertek maximizes customer experience, drives new revenue and manages costs with powerful solutions that combined industry-leading talent, proven solutions and robust processes

Key Person:
Ron Hruby,
VP Cybersecurity

Website:
vertek.com

Vertek

Protect Your Customers Now!

Ron Hruby

An increasing number of businesses are looking for fully managed Security Information Event Management (SIEM) solutions over investing in the technology itself. While there are numerous products available in the market today all claiming to be easy to implement and manage, internal IT teams simply do not have the time to implement, leverage all features, manage or effectively tune and monitor the noise these products tend to generate. More businesses are turning to Managed Service Providers (MSPs) for managed security solutions, especially mission critical security products such as SIEM. However, many MSPs are not set up or staffed to make the transition to become a fully functioning 24/7 Managed Security Services Provider (MSSP). In such a scenario, Vertek is uniquely positioned to provide bolt-on 24/7 Managed SIEM and Security Operations Center (SOC) services. With a 100 percent channel-driven sales model, Vertek enables Referral Partners, Agents and Resellers to offer these highly specialized services to their customer base. The company's Managed Threat Intelligence (MTI) offering is a 24/7 SIEM and SOC-as-a-Service (SOCaaS) solution, that puts enterprise-class security visibility and compliance reporting within easy reach of IT departments that need to do more with less. “Unlike ordinary SIEM products or providers that simply notify you of every alarm, we eliminate the noise and help you prioritize and mitigate the threats that put your businesses at risk- it's one of core values that we bring,” says Ron Hruby, VP of Cybersecurity at Vertek.

> “We eliminate the noise and help you prioritize the threats that put your business at risk”

By leveraging Vertek's MTI service, partners and customers can instantly add world-class security engineers, processes, and tools for comprehensive IT security protection. Vertek continuously collects, aggregates, and monitors security data across the network, comparing data to known cyber threats and alerting IT staff to security gaps, vulnerabilities and network infiltrations. Along with the benefits of a SIEM, Vertek contributes a massive number of Indicators of Compromise (IOCs) to the Open Threat Exchange (OTX) daily, providing them a competitive advantage to detect and respond to new and emerging threats. When a threat or an alarm is detected, Vertek responds with recommended remediation guidance to mitigate the risk. “We offer custom threat feeds, perform vulnerability scanning and conduct monthly security reviews where we digest security reports and statistics that we use to help customers align, track and prioritize security concerns, as well as meet compliance initiatives.” says Hruby.

Today, Vertek leverages AT&T Cybersecurity's AlienVault® Unified Security Management® (USM) platform to deliver MTI, which combines powerful SIEM and log management capabilities with other essential security tools—including asset discovery, vulnerability scanning and intrusion detectionto give centralized security monitoring of networks and endpoints across your cloud and on-premises environments–all from a single pane of glass.

An interesting case study is that of an MSP that wanted to protect not only themselves but also the data and assets of its customers. They initially approached Vertek to collaborate on threat identification and response scenariossuch as unauthorized attempts to gain access to customer information or attempts to exfiltrate data out of one of their many datacenters. The MSP was also interested in gaining an independent view relative to their overall security posture. By Vertek fulfilling all these requirements, not only was the MSP able to respond to its customers' inquiries regarding its own security posture, but they were also able to go to market with a custom MDR (Managed Detection Response) solution to offer powerful security services to their customers.

As a recognized partner of AT&T Cybersecurity and a Master AlienVault provider, Vertek is moving ahead to expand its business with strategic partnerships and new customers. From the product perspective, Vertek is always evaluating other security products to add to their SOCaaS portfolio to solve additional security use cases and fill niche markets. ES