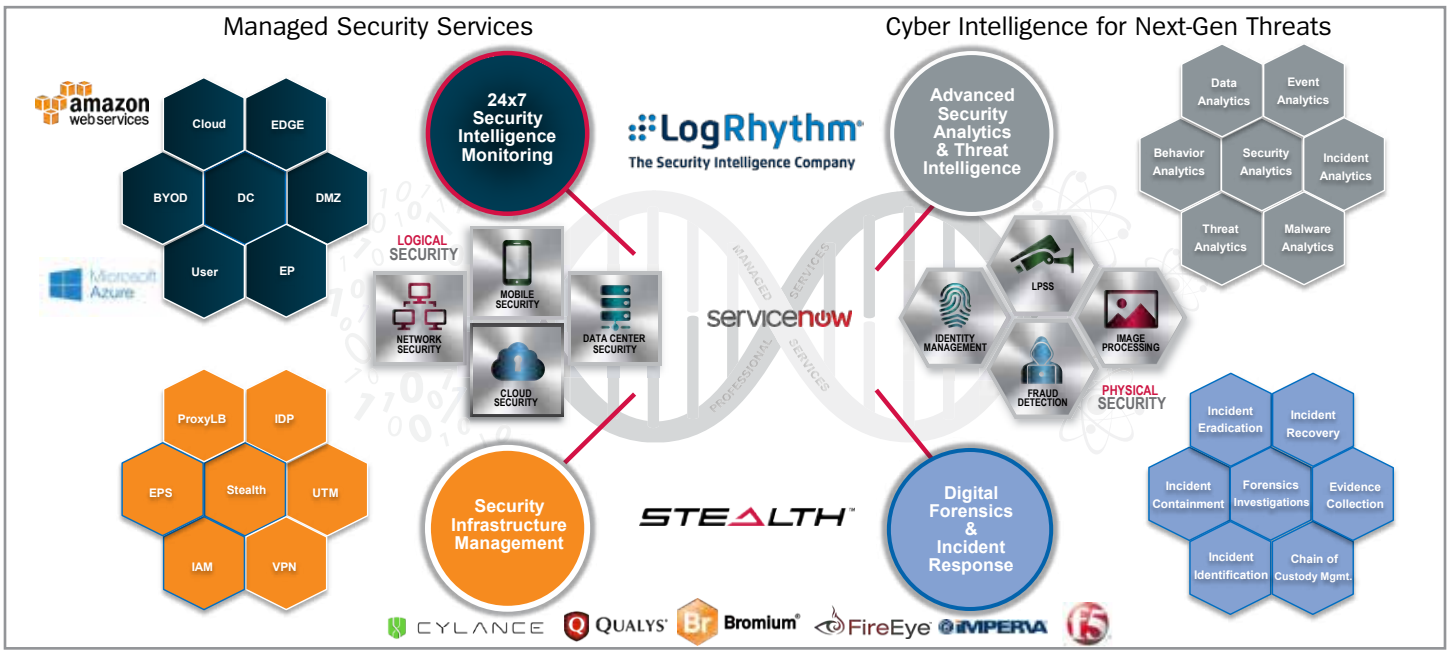
UNISYS

LogRhythm

Unisys Managed Security Services Featuring LogRhythm

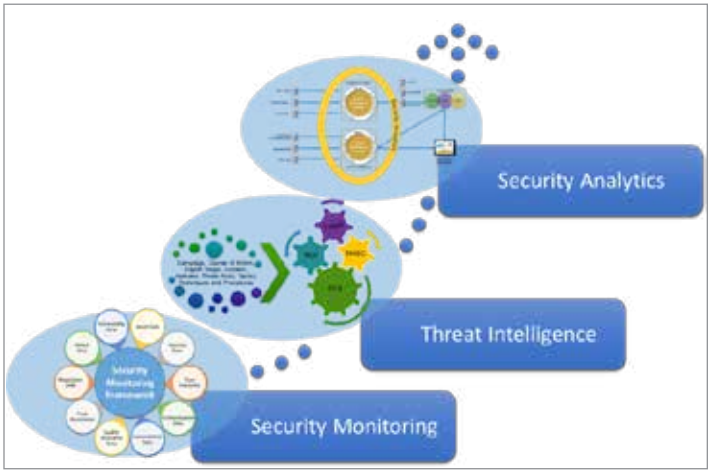


Enterprise networks are large, highly complex, and overwhelmed with large volumes of logs. Most of those logs usually contain noise, which makes it harder to identify critical security events. At the same time, regulatory and compliance requirements are getting more challenging and demanding. Trying to keep pace, many enterprises are investing in expensive and complex solutions and combinations of technology, while often lacking the resources to become situationally aware.

Your security is as effective as your security intelligence. Overcoming sophisticated security challenges needs well fabricated security intelligence from a number of technologies and threat sources. To meet these requirements, Unisys amassed multiple key SIEM ingredients powered by LogRhythm technology.

Security Monitoring

Unisys SIEM services, are designed to support our clients across multiple domains including log management, event analytics, IT Operations, IT GRC, and risk management. Each service is flexibly tailored to the existing environment of each client,



ranging from simple log management to a fully-fledged security monitoring solution covering the entire holistic attack surface.

LogRhythm's best-in-class SIEM collects logs from across the customer environment, providing a single pane of glass for security monitoring. The platform then normalizes these logs to extract risk intelligence in an automated manner. This processing and enrichment enables real-time threat detection and streamlines manual analysis.

Threat Intelligence

LogRhythm's AI Engine enables Unisys to process threat intelligence feeds from commercial and open-source threat feeds, as well as internal honeypots. Using LogRhythm we make threat intelligence actionable, using it to predict upcoming threats and aid manual analysis efforts.

Leveraging threat intelligence, our clients can:

- See attacks in context
- Detect threats that would otherwise go unnoticed

Advanced Security Analytics

Security analytics with valuable threat intelligence feeds are the functional building blocks for our next generation of security monitoring services. Our continuous engagement with LogRhythm Labs helps us deliver advanced security analytics that solve real use cases, including:

- **User-based threats**: insider threats, account takeover, privilege abuse and misuse, and more
- **Network-based threats:** malware command and control communication, remote zero-day attacks, network data exfiltration, and more
- **Endpoint-based threats:** advanced local malware detection, suspicious processes, local data exfiltration, Cloud data abuse, and more

Incident Response & Orchestration

For this we:

1. Centralize access to data from across your IT environment;
2. Search massive data sets with unprecedented speed and precision using unstructured or contextual search;
3. Orchestrate and automate incident response using LogRhythm's collaborative case management workflows;
4. Automate incident investigation and remediation with pre-staged SmartResponse™ automation actions.

Why Unisys?

Staying ahead of the bad guys means monitoring and analyzing huge data sets of security logs from a multitude of systems. This effort is highly complex, and expensive, requiring 24x7 real time monitoring in a world with a massive shortage of qualified cybersecurity resources. Further, Enterprises are finding out the hard way that just implementing SIEM systems do not yield benefits until these systems are tuned to their to specific computing environment needs.

With decades of multi-industry and global Managed Security experience, Unisys offers a combination of best in class SIEM architecture with sophisticated event analytics. Unisys also has world-class expertise creating "information visibility" and compliance solutions for our clients.

Enterprise clients benefit from a highly skilled team of security experts offering protection within our seven global Security Operations Centers (SOCs). These SOCs provide real-time, 24x7 monitoring capabilities based on the "follow-the-sun" model.

Unisys managed SIEM facilitates enterprise-wide event collection to detect client security events, and to ensure they are correlated and responded to proactively.

Complementing Services and Product Recognition: Unisys Industry Recognition

LogRhythm Industry Recognition

Contact Us:

It's time to try a fresh approach to your managed security services, from a provider that's already solved many of the problems you face today. To get more information or to schedule a discussion and demonstration, please contact your Unisys sales executive or visit www.unisys.com/security.

For more information visit www.unisys.com/security

Printed in the United States of America 10/16 16-0505