securonix

Persistent

CASE STUDY

Persistent Systems Transforms Security Posture with Securonix

securonix

Persistent

CASE STUDY

Persistent Systems Transforms Security Posture with Securonix

About Persistent Systems

With over 23,000 employees located in 21 countries, Persistent Systems (BSE & NSE: PERSISTENT) is a global services and solutions company delivering Digital Engineering and Enterprise Modernization. As a participant of the United Nations Global Compact, Persistent is committed to aligning strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, as well as taking actions that advance societal goals. With 268% growth since 2020, Persistent is the fastest-growing Indian IT Services brand according to Brand Finance.
www.persistent.com

"Securonix went above and beyond. Their team seamlessly guided our deployment and even built some custom use cases to fit our unique needs. It's a true partnership, not just a vendor relationship."

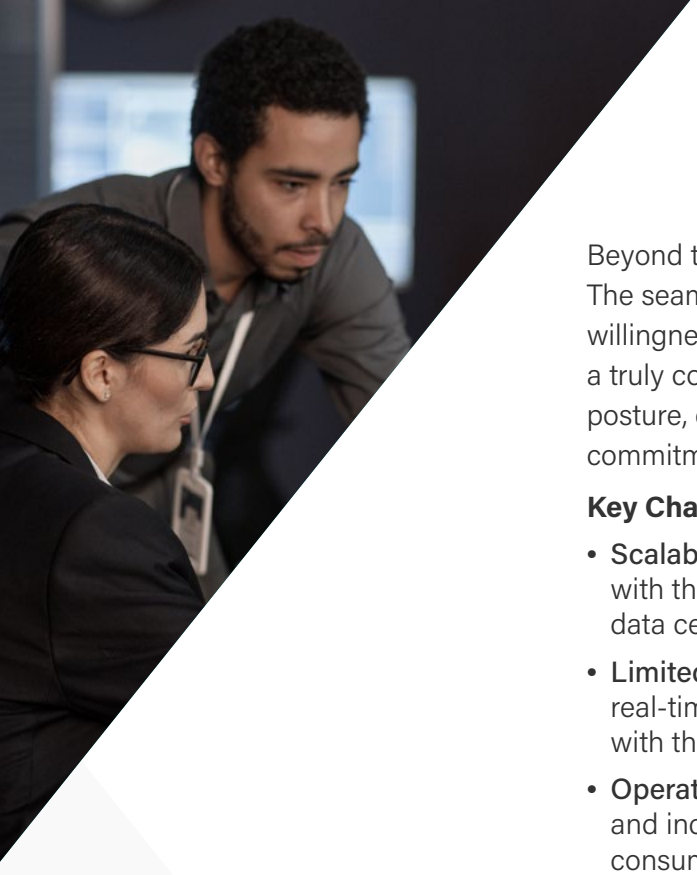
– **Avinash Dharmadhikari**
CISO, Persistent Systems

The Challenge: Managing security for a rapidly growing global IT services leader with on-prem and cloud workloads across diverse geographies. Legacy SIEM was causing administrative overhead, scalability issues, and limited detection capabilities.

Persistent Systems, a global Digital Engineering and Enterprise Modernization leader, navigates the complex digital landscape for clients across diverse industries like banking, healthcare, and life sciences. As businesses become increasingly reliant on data and interconnected ecosystems, cyber security stands as a non-negotiable cornerstone of their operations. With a geographically dispersed workforce and sprawling IT infrastructure, ensuring data integrity and threat mitigation becomes a multifaceted challenge.

The limitations of their legacy on-premises SIEM solution became increasingly apparent. Administrative overheads, scalability constraints, and limited detection capabilities hampered their ability to effectively monitor and protect their vast digital territory. Persistent needed a modern, cloud-based security solution that could provide real-time visibility, proactive threat detection, and streamlined incident response capabilities.

Enter Securonix Unified Defense SIEM. Armed with a potent combination of cloud-native scalability, robust UEBA features, and an integrated SOAR platform, Securonix transformed Persistent's security posture. The 100% workload coverage eliminated blind spots across on-prem, cloud, and data center environments, granting comprehensive real-time visibility. Securonix UEBA's granular user activity insights shed light on anomalies like suspicious logins across diverse locations, empowering proactive threat prevention for their global workforce. The automated incident creation capabilities of Securonix SOAR further streamlined operations, reducing manual tasks and accelerating response times.



Beyond technology, the partnership with Securonix proved invaluable. The seamless deployment support, coupled with the engineering team's willingness to develop custom features and OOTB use cases, solidified a truly collaborative effort. Persistent now enjoys a more robust security posture, empowered by Securonix's continuous innovation and unwavering commitment to customer success.

Key Challenges

- **Scalability bottlenecks:** Their legacy on-prem SIEM struggled to cope with their rapid growth and diverse IT infrastructure across cloud and data centers, creating blind spots and hindering effective monitoring.
- **Limited threat detection:** A lack of advanced features like UEBA and real-time anomaly detection left them vulnerable to sophisticated threats, with their previous platform lagging behind their evolving security needs.
- **Operational inefficiencies:** Manual configuration, patch management, and incident response hampered their security team's productivity, consuming valuable time and resources.
- **Hybrid Cloud Monitoring:** Their legacy solution was unable to onboard cloud data sources and bring both on-prem and cloud visibility on a single pane of glass.

Solution

Securonix Unified Defense SIEM, adopted for its cloud-based architecture, scalability, UEBA, SOAR, and real-time visibility.

Results

- **100% workload coverage:** Eliminated blind spots across on-premises, cloud (AWS, Azure, Google, Oracle), and data center environments.
- **Enhanced detection and visibility:** Improved real-time detections with features like UEBA, identifying anomalies like multiple failed logins or admin access at odd hours.
- **Reduced manual effort and faster response:** Streamlined operations with the included OOTB Securonix SOAR content including building 16 custom playbooks to increase automation and reduce manual effort.
- **Enhanced threat intelligence:** Enabled real time actionable insights through connectors and integrated threat feeds from other tools into Securonix.

"The partnership between Securonix and Persistent Systems (PSL) is strategic for us, elevating PSL's security operations posture with our Unified Defense SIEM (UDS) platform is a testimony to our commitment to making enterprises resilient to advanced threats."

– Harshil Doshi
Sales Director, India

Key Takeaways

- Securonix provided a modern, scalable SIEM solution to address Persistent's growth and security challenges
- UEBA capabilities offered deeper user activity insights and anomaly detection for improved threat prevention
- Real time visibility across on-prem and multi-cloud workloads enabled more accurate and timely detections
- SOAR automation reduced manual tasks and accelerated incident response
- Integration with external threat feeds enriched Securonix with valuable context for actionable insights
- Strong partnership with Securonix, including deployment support, custom use case development, and ongoing roadmap discussions, facilitated a successful implementation and continuous improvement

Persistent immediately had access to real-time visibility, proactive threat detection, and faster response capabilities, thanks to Securonix.

"Coverage is important because what you cannot see, you cannot detect. In a very short span of time, we were able to achieve 100% coverage of all our use cases and requirements with Securonix."

– Avinash Dharmadhikari
CISO, Persistent Systems

About Securonix

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation, and response (TDIR) solution built with a highly scalable data cloud and a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats.

For more information visit securonix.com