OBSERVE NOW | kaspersky

Presents

The Intelligence Edge:

HeartBeat of Modern Security Operations

Date: 9th August 2024
Venue: Bengaluru

ObserveNow and Kaspersky hosted an exclusive roundtable discussion on “The Intelligence Edge: Heartbeat of Modern Security Operations” on August 9, 2024, in Bengaluru. The event primarily aimed to explore the significance of threat intelligence and the future of Security Operations Centers (SOCs).

The session delved into the growing necessity of threat intelligence in safeguarding organisations and individuals, highlighting the crucial role of integrating threat intelligence into SOCs. This integration transforms raw data into actionable insights, enabling SOCs to predict and mitigate cyber threats. However, it also presents challenges that organisations need to overcome to optimise its effectiveness.

Taniya Tikoo, Editor-in-Chief and Co-founder of ObserveNow, initiated the discussion by welcoming all the leaders and providing an overview of the topic. She emphasized the significance of Threat Intelligence and the evolution of future SOCs.

Additionally, Taniya presented data on various threats, highlighting the urgency of advancing threat intelligence capabilities in response to the alarming statistics.

Session Attendees: Cybersecurity Leaders

- **Satish Kumar Dwibhashi,** CISO, KreditBee
- **Kamesh Babu R,** CISO, Global Head of IT and Cybersecurity, Subex
- **Surendra Nemani,** BISO and Head Of Security, Flipkart's ClearTrip, Flipkart
- **Saksham Tushar,** Head of Security Operations & Threat Detection Engineering, CRED
- **Chandra shekhar,** Head of information security, Porter
- **Krishnendu Dutta,** Head of Information Security, Decathlon Sports India
- **Naseem Halder,** Head of Cyber Security and Compliance Slice
- **Sourabh Kulkarni,** Senior Cyber Security Engineer, Payu
- **Archit Rajesh,** Senior Vice President, FirstMeridian
- **Sanu Kumar Gupta,** Engineering Leader, MEESHO
- **Ram sandesh,** Flipkart

The speakers emphasised the critical role of effective threat intelligence in enhancing SOC capabilities. They discussed the necessity of real-time, accurate threat feeds and the challenges posed by their improper integration, which can overwhelm security teams. This article explores best practices for collecting, preventing, detecting, and responding to threats to improve overall security posture.

SOC teams must adopt a proactive stance by utilising high-quality threat feeds, fostering community collaboration, and effectively deploying Indicators of Compromise (IoCs). Additionally, conducting contextual analyses of threat data is essential for bolstering defences against evolving cyber threats.

With the abundance of threat intelligence, organisations may struggle to prioritise which vulnerabilities require immediate attention. Improperly leveraging threat intelligence can lead to significant issues. For emerging threats, benchmarking against CVSS scores is recommended to assess potential risks and identify SOC errors. Proper classification of threats remains a crucial element in managing cybersecurity effectively.

Event Glimpses: