A REPORT ON

Workshop on Security Monitoring

Date: 12th and 13th July 2024
Venue: Cyber Security lab, EB – 1st floor, Silver Oak University

Introduction:

Extolling the **'Workshop on Security Monitoring'**, the **Department of CSE-CS, SOCET** with **Silver Oak University IEEE Computer Society Student Branch Chapter** and **SecureOps at Silver Oak University**. This workshop focused on developing attendees in the field of cybersecurity by covering topics such as **'Security Monitoring Tools and Technologies'**, **'Splunk'**, and **'Training on Incident Response'** to prepare them for their future endeavours.

About the speaker:

The Session was conducted by expert professors:

1. **Prof. Harshita Makwana:** Assistant professor, Department of CSE-CS, SOCET
2. **Prof. Sunny Mesuriya:** Assistant professor, Department of CSE-CS, SOCET

About the event:

Date: - 12th & 13th July, 2024
Time: - 3:00 PM to 5:00 PM
Venue: - Cyber Security lab, EB – 1st floor, Silver Oak University
Participants: - 86

Day 1

The workshop on security monitoring began with a buzz of excitement as attendees filled the lab with vibrant enthusiasm and positive energy. Prof. Harshita Makwana kicked off the session by highlighting the critical importance of security monitoring, covering essential aspects of the Security Operation Centre such as 24/7 continuous monitoring and proactive security management. The discussion then shifted to alert management, distinguishing between actual and lower management. Prof. Makwana delved into key topics including infrastructure threat response, log reporting and monitoring, and vulnerability assessment, ensuring participants comprehensively understood the security monitoring landscape.

Prof. Sunny Mesuriya broadened the attendees' world of cloud security, beginning with log collection and reporting to provide real-time visibility into potential threats. By leveraging the knowledge acquired from research and development, attendees identified and responded to threats more effectively and also examined the core of data security. The speaker then introduced members to the heart of security monitoring, SIEM systems.

Day 2

Day 2 commenced with Prof. Sunny Mesuriya, guiding participants through the advanced cybersecurity frameworks and strategies, from ping checking to bridge checking the network and installations. Attendees then set up forwarders and performed comparisons, engaging in hands-on exercises using Security tools like Argus, POF, Splunk, and Nagios, reinforcing the session's lessons.

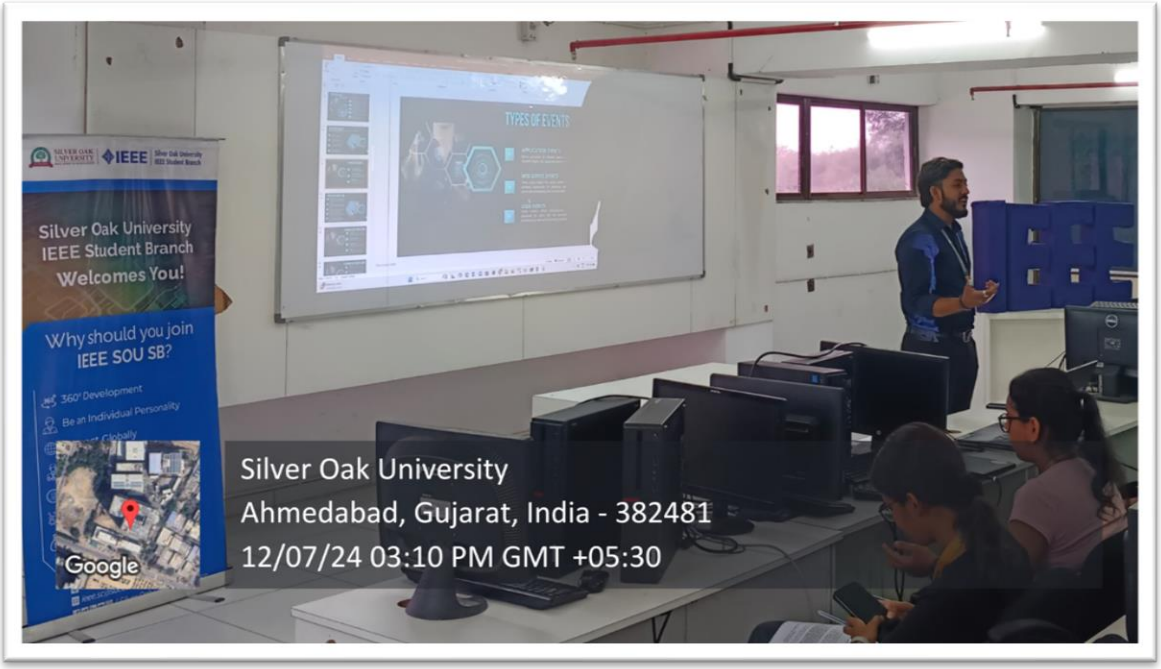
Prof. Harshita Makwana provided comprehensive guidance on monitoring security incidents, understanding standards with its policies related to unauthorized access and the CIA triad which truly enhanced the members' knowledge. The discussion included insights into SIEM architecture and operations, covering log management architecture, details and lists, and practical demonstrations of generating alerts.

Conclusion

The two-day **"Workshop on Security Monitoring"** concluded covering crucial topics of SOC operations, alert management, log monitoring, and vulnerability assessment. Participants gained hands-on experience focused on advancing cybersecurity frameworks, including ping checking, bridge checking, and SIEM architecture giving participants an overview of security incident management, log management, and alert generation, equipping them with practical skills and valuable insights.

This endeavour was successful under the guidance of Dr. Satvik Khara, Dean of Diploma Engineering at Silver Oak University (SOU); Head of the Department of Computer Engineering at SOCET; IEEE Senior Member; Chairperson of SIGHT, IEEE Gujarat Section; Secretary of the Computer Society, IEEE Gujarat Section; and Founding Member of the Silver Oak University IEEE Student Branch, who provided indispensable guidance and supported the Student Branch towards excellence.

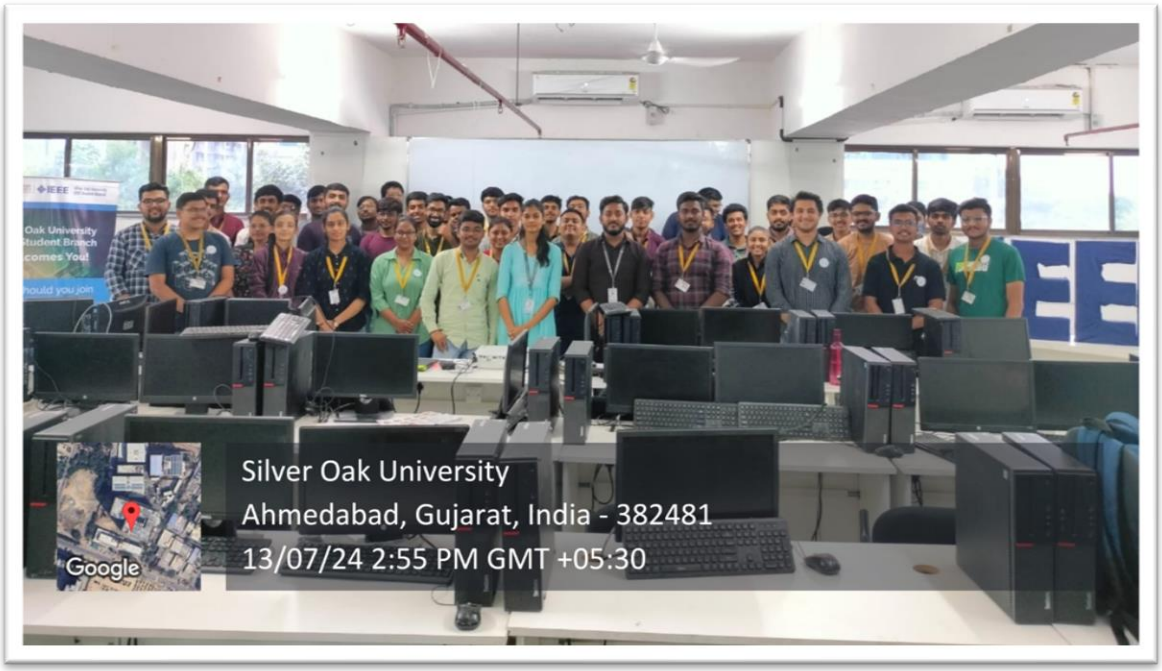
Some glimpses of the event:



Prof. Mesurya elaborating on event logs

Attendees gaining hands-on experience

Prof. Makwana solving doubts with a proactive method



Successful conclusion of the event with a group photo