Welcome To The 10th Annual Hacking Conference
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!
WHY YOUR SEIM TOOL IS NOT ENOUGH

ALTERNATIVE APPROACHES TO IDENTIFYING AND REACTING TO THREATS

ROBERT KIRTLEY

NOVEMBER 6, 2023
OVERVIEW

• Introduction/Definitions
• Evolution of SIEM - history of the SIEM
• Where we are today - XDR, EDR, MDR
  • EDR
  • XDR
  • MDR
• Future Ecosystem
INTRODUCTION/DEFINITIONS

SEIM

MDR

EDR

XDR
HISTORY OF THE SEIM

- The integration of dealing with information and events concurrently
- More is not always better
- Integration of analytics
- Evolution – moving from reactive to proactive posture
EVOLUTION OF SECURITY TOOLS

• EDR
• XDR
• MDR
EDR

• Endpoint-focused
• The evolution of traditional AV
• NGAV
• Not wholistic across the environment
XDR

• Evolution of MDR
• A complement to SEIMs
• Orientation – bottom up vs top down
MDR

• EDR/XDR + Services
• Human and AI assisted threat hunting
• External/Internal linkages
• Managed remediation
IS THERE A RIGHT ANSWER?

• The lawyer’s answer…. It depends

• Considerations include:
  • Risk profile
  • Business requirements
  • Network/Infrastructure profile
  • Staffing
  • Budget
THE FUTURE

• AI and ML-Enabled XDR
• New attack surfaces
• Integration with zero-trust factors
• New authentication tools
• Acceleration of cloud computing
Welcome To The 10th Annual Hacking Conference