# Mini SOC Cybersecurity

CP422031 Introduction to Cybersecurity

ศ.ดร.จักรชัย โสอินทร์
ผศ.ดร.สาธิต กระเวนกิจ

## หลักการและเหตุผล

SOC เป็นศูนย์กลางในการป้องกันและรับมือกับภัยคุกคามไซเบอร์ช่วยลดความเสี่ยงต่อทรัพย์สินดิจิทัล ข้อมูล และความน่าเชื่อถือขององค์กร ทำให้องค์กรมั่นคงในโลกดิจิทัลที่ซับซ้อนและเปลี่ยนแปลงรวดเร็ว

## วัตถุประสงค์

1.Learning (ศึกษา) – พัฒนาความเข้าใจและทักษะด้านความปลอดภัยไซเบอร์ ทั้งภาคทฤษฎีและปฏิบัติ รวมถึงพื้นฐาน SOC, การตอบสนองต่อเหตุการณ์ และเตรียมความพร้อมสู่สายอาชีพด้านความปลอดภัยไซเบอร์ เช่น SOC Analyst และ Threat Hunter
2.Customizing (ติดตั้ง/ปรับแต่ง) – ปรับแต่ง SOC ให้เหมาะสมกับภัยคุกคาม โดยติดตั้งเครื่องมือเฝ้าระวัง ออกแบบให้ใช้งานง่าย และสามารถตอบสนองต่อเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพ

## ขอบเขตการศึกษา

1. พื้นฐาน SOC และบทบาทในการรักษาความปลอดภัยไซเบอร์
2. การตอบสนองต่อเหตุการณ์ (Incident Response)
3. การติดตั้งและใช้งานเครื่องมือเฝ้าระวังภัยคุกคาม
4. การปรับแต่ง SOC ให้เหมาะสมและจัดการผ่าน Dashboard
5. เตรียมความพร้อมสู่สายอาชีพด้านความปลอดภัยไซเบอร์

## เครื่องมือที่ใช้งาน

1. Elasticsearch
2. Kibana
3. Metasploit

## อ้างอิง

https://www.youtube.com/playlist?list=PLG6KGSNK4PuBb0OjyDIdACZnb8AoNBeq6

## สมาชิกกลุ่ม

1.ปวรุตม์ หงษ์ชุมแพ 663380465-9
2. ปัณณวัฒน์ กุลวงษ์ 663380117-2
3.วันเฉลิม ภักดี 663380133-4
4.รัชพล กันโฮมภู 663380126-1
5.บวรภัค ทิพม้อม 663380115-6
6.นายวริทธิ์ธร ลิขิตวงศ์ขจร 663380132-6