



หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการและเทคโนโลยีดิจิทัล (DST)

(3) กลุ่มวิชาความมั่นคงปลอดภัย

คำอธิบายรายวิชากลุ่มวิชาเลือกเฉพาะด้าน

จำนวนหน่วยกิต (ทฤษฎี - ปฏิบัติ - คำนวณ)

ทสวด 351 ความมั่นคงปลอดภัยทางไซเบอร์ขั้นสูง 3 (2 - 2 - 5)

ITDS 351 Advanced Cybersecurity

รายวิชาที่ต้องเรียนมาก่อน : ทสวด 271

รายวิชาที่ต้องเรียนควบคู่กัน : ไม่มี

ภัยคุกคามและการโจมตีทางไซเบอร์ ความมั่นคงปลอดภัยทางไซเบอร์ที่รวมถึง ดีเอชซีพี แอลดีบี การควบคุมโดเมน ความมั่นคงปลอดภัยเครือข่ายทั้งแบบสายและไร้สาย อาทิจี ไฟร์วอลล์ เครือข่ายระยะใกล้แบบเสมือน ดับเบิลยูพีเอส การควบคุมการเข้าถึงฐานข้อมูล ความมั่นคงปลอดภัยของคลาวด์ ความมั่นคงปลอดภัยของแอปพลิเคชันเว็บ เทคนิคการโจมตีทางไซเบอร์ผ่านการโจมตีเครือข่าย เช่น การดักจับข้อมูล การทำให้โปรโตคอลอาฟเป็นพิษ การปลอม และการปลอมตัวของแอคเซสพอยท์ ความมั่นคงปลอดภัยของระบบอาทิจี การเข้าถึงแบบไม่มีสิทธิ์ และการเข้าถึงเพื่อโจมตี การโจมตีแอปพลิเคชันเว็บตามที่กำหนดในโอวาส์ฟ 10 อันดับแรก การโจมตีทางวิศวกรรมสังคม เช่น การหลอกลวงทางอีเมล และการปลอมบัญชี มัลแวร์ที่รวมถึงไวรัส โทรจัน ตัวหนอน โปรแกรมเรียกค่าไถ่ ภัยคุกคามยืนยาวขั้นสูง การโจมตีแบบมีจรรยาบรรณ การประเมินจุดอ่อนพื้นฐาน เครื่องมือและการทดสอบการเจาะระบบ กรณีศึกษาจริงของการโจมตีทางไซเบอร์พร้อมบทเรียนที่ได้รับ

Cyber threats and attacks; the cybersecurity including DHCP, LDAP, the domain controller; the network security both wired and wireless such as Firewall, VLAN, WPA2; the database access control; cloud security. web application security; cyber attack techniques via network attacks such as sniffing, ARP poisoning, spoofing, and the rouge access point; system attacks such as the unauthorized access and exploitation; web application attacks according to the OWASP top 10; social engineering attacks such as phishing and fake accounts; malware including virus, trojan, worm, ransomware; advance the persistent threat (APT); ethical hacking; the basic vulnerability assessment, penetration testing and tools; real case studies of cyber-attacks with lesson learns

ทสวด 352 การพัฒนาซอฟต์แวร์อย่างปลอดภัย 3 (2 - 2 - 5)

ITDS 352 Secure Software Development

รายวิชาที่ต้องเรียนมาก่อน : ทสวด 271

รายวิชาที่ต้องเรียนควบคู่กัน : ไม่มี

วงจรชีวิตของการพัฒนาซอฟต์แวร์และระบบอย่างปลอดภัย ลักษณะความเสี่ยงและช่องโหว่ของระบบและซอฟต์แวร์ที่พบบ่อย การกำหนดความต้องการด้านความมั่นคงตามมาตรฐานความปลอดภัยที่เกี่ยวข้อง อาทิ ISO27001 และ PCIDSS กฎหมายที่เกี่ยวข้อง รายการตรวจสอบด้านความมั่นคงของการพัฒนาซอฟต์แวร์ กระบวนการวิเคราะห์และออกแบบ หลักการป้องกันที่ช่วยให้ซอฟต์แวร์มีความปลอดภัยและน่าเชื่อถือซึ่งรวมถึง การเป็นความลับ ความบริสุทธิ์ ความพร้อมใช้งาน การพิสูจน์ตัวตน การกำหนดสิทธิ์ การทำรายการบัญชี และการไม่สามารถปฏิเสธได้ หลักการออกแบบซอฟต์แวร์อย่างปลอดภัยที่รวมถึง การกำหนดสิทธิ์ต่ำสุด การแบ่งหน้าที่ การป้องกันอย่างลึก การล้มแบบปลอดภัย กลไกที่เหมือนกันน้อยสุด การกำจัดจุดอ่อนเดียว กรณีการใช้งาน กรณีการใช้งานที่ไม่ถูกต้อง การตรวจสอบส่วนที่ถูกโจมตี กระบวนการการพัฒนาและการเขียนโปรแกรม รวมถึงการเขียนแบบมั่นคง การตรวจดูต้นฉบับของโค้ด มาตรฐานการทดสอบแบบมั่นคง การประเมินจุดอ่อน และการจัดการจุดอ่อน กระบวนการการนำไปใช้งาน รวมถึงการเห็นชอบให้ใช้งาน และการจัดการการเปลี่ยนแปลง กระบวนการปฏิบัติที่รวมถึง การตรวจสอบและตอบสนองความมั่นคงอย่างต่อเนื่อง ขั้นตอนการยกเลิกการใช้งาน

The secure software and system development life cycle; risk characteristics and often system and software vulnerabilities; security requirements according to related security standards such as ISO27001 and PCIDSS; related laws; the development security checklist; analysis and design phases; protection principles to help software secure and reliable including confidentiality, integrity, availability, authentication, authorization, accountability, and nonrepudiation; security design principles including the least privilege, the separation of duties, the defense in depth, the fail safe, the least common mechanism, the elimination of the single point of failure, use cases, misuse cases, the attack surface validation, the implementation and coding phases including the secure coding, the source code review, security testing standards, the vulnerability assessment, and the vulnerability management; the deployment phase including the deployment approval and change management; the operation phase including the continuously security monitoring and response; the disposal phase

ทสวด 353 นิติวิทยาศาสตร์ดิจิทัลพื้นฐาน 3 (2 - 2 - 5)

ITDS 353 Fundamentals of Digital Forensics

รายวิชาที่ต้องเรียนมาก่อน : ทสวด 271

รายวิชาที่ต้องเรียนควบคู่กัน : ไม่มี

การตรวจสอบดิจิทัล การรวบรวมหลักฐานดิจิทัล การเก็บรักษาหลักฐานดิจิทัล ฮาร์ดแวร์คอมพิวเตอร์ การวิเคราะห์ระบบไฟล์, การกู้คืนไฟล์ การวิเคราะห์หน่วยความจำ เครื่องมือวิเคราะห์นิติวิทยาศาสตร์ดิจิทัล การสร้างรายงานนิติวิทยาศาสตร์ดิจิทัล เครื่องมือซอฟต์แวร์สำหรับนิติวิทยาศาสตร์ดิจิทัล

Digital investigations, digital evidence collections, digital evidence preservations, the computer hardware, the file system analysis, the file recovery, the memory analysis, digital forensic analysis tools, digital forensic reports, software tools for digital forensics

ทสวด 354 การจัดการความเสี่ยงทางไซเบอร์และการปฏิบัติการ 3 (3 – 0 – 6)

ITDS 354 Cyber Risk Management and Operation

รายวิชาที่ต้องเรียนมาก่อน : ทสวด 271

รายวิชาที่ต้องเรียนควบคู่กัน : ไม่มี

แนวคิดการจัดการความเสี่ยง การประเมินความเสี่ยง การวิเคราะห์ความเสี่ยง ระบุภัยคุกคามและความเสี่ยง การตอบสนองความเสี่ยง การเลือกมาตรการตอบโต้ การประเมินการควบคุมความปลอดภัย การตรวจสอบกรอบการบริหารความเสี่ยง รายงานการวิเคราะห์ความเสี่ยง

Risk management concepts; risk assessment; risk analysis; identifying threats and vulnerabilities; risk response; countermeasure selection; the security control assessment; monitoring; risk management frameworks; risk analysis reporting

ทสวด 355 การตรวจสอบด้านเทคโนโลยีสารสนเทศ 3 (2 – 2 – 5)

ITDS 355 IT Auditing

รายวิชาที่ต้องเรียนมาก่อน : ทสวด 271

รายวิชาที่ต้องเรียนควบคู่กัน : ไม่มี

สิ่งแวดล้อมทางเทคโนโลยีสารสนเทศ การทำงานของการตรวจสอบภายในและภายนอก บทบาทของการตรวจสอบด้านเทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศแบบมืออาชีพ กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ กระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศที่ประกอบด้วย การวางแผน การจัดลำดับ การจัดงบประมาณ ขอบเขต ทีมงาน การทำงาน และเส้นตาย เครื่องมือและเทคนิคที่ใช้ในการตรวจสอบด้านเทคโนโลยีสารสนเทศ การกำกับดูแลและกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ความเสี่ยงและการควบคุม การจัดการควบคุมการเปลี่ยนแปลง การปฏิบัติการในระบบสารสนเทศ ความมั่นคงปลอดภัยของสารสนเทศ การจัดการระบบ และการรับเหมาช่วงต่อ การทำเอกสาร การรายงานและการนำเสนอ กรณีศึกษา

The IT environment; functions of internal and external audits; roles of IT auditing; professional IT auditing; legislation related to IT; the IT audit process: planning, scheduling, budgeting, scope, team, tasks and deadlines; tools and techniques used in auditing IT; IT governance and strategy; risks and controls; the change control management; information systems operations; the information security; systems acquisition and outsourcing; documentation; reporting and presentation; case studies

ทสวด 356 ความมั่นคงปลอดภัยเชิงปฏิบัติ

3 (0 - 6 - 3)

ITDS 356 Practical Cybersecurity

รายวิชาที่ต้องเรียนมาก่อน : ทสวด 271

รายวิชาที่ต้องเรียนควบคู่กัน : ไม่มี

การใช้เครื่องมือซอฟต์แวร์ในการติดตั้งเครือข่ายสื่อสารจำลองแบบสายและไร้สาย การจำลองเหตุการณ์และการทดสอบหาจุดอ่อน การรวบรวมข้อมูลเชิงความลับ การดักจับข้อมูลจราจรของเครือข่าย การใช้เครื่องมือซอฟต์แวร์เพื่อทดสอบการเข้าถึงฐานข้อมูลและเพื่อหาจุดอ่อนของแอปพลิเคชันเว็บ เทคนิคในการตรวจจับการโจมตีเชิงวิศวกรรมสังคม การใช้เครื่องมือซอฟต์แวร์ในการทดสอบเจาะระบบ

Using the software tools to install the wire and wireless network communication; simulating and testing for vulnerability; intelligence gathering; network traffic information sniffing; using the software tools for testing the database accessibility and for finding the vulnerability of the web application; the techniques to identify the social engineering attacks; using the software tools for penetration testing