

กระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์ กรณีเว็บไซต์พนัน

Incident Response Process in case gambling web



ที่มาและความสำคัญ



- ภัยคุกคามทางไซเบอร์ที่รุนแรงแก้ปัญหาด้วยแผนรับมือภัยคุกคามทางไซเบอร์
- การโจมตีด้วยการแก้ไขเปลี่ยนแปลงเว็บไซต์เกิดขึ้นบ่อย
- ปัญหาเว็บไซต์ถูกโจมตีให้เป็นเว็บพแนอนออนไลน์เกิดมากที่สุดในสถาบันการศึกษา



วัตถุประสงค์

- เพื่อให้มีกระบวนการรับมือภัยคุกคามทางไซเบอร์
- เพื่อแก้ไขเว็บไซต์ที่ถูกโจมตี
- เพื่อป้องกันไม่ให้เกิดการโจมตีซ้ำ



งานวิจัยที่เกี่ยวข้อง

- ภัยคุกคามด้านไซเบอร์
- การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์
 - การบริหารความเสี่ยง
 - การใช้กรอบมาตรฐาน NIST
 - กรอบมาตรฐาน NIST 5 ขั้นตอน
 - Identify Protect Detect Response Recovery
- การบริหารจัดการการรับมือภัยคุกคามไซเบอร์
- กระบวนการจัดการการรับมือภัยคุกคามไซเบอร์



กระบวนการ

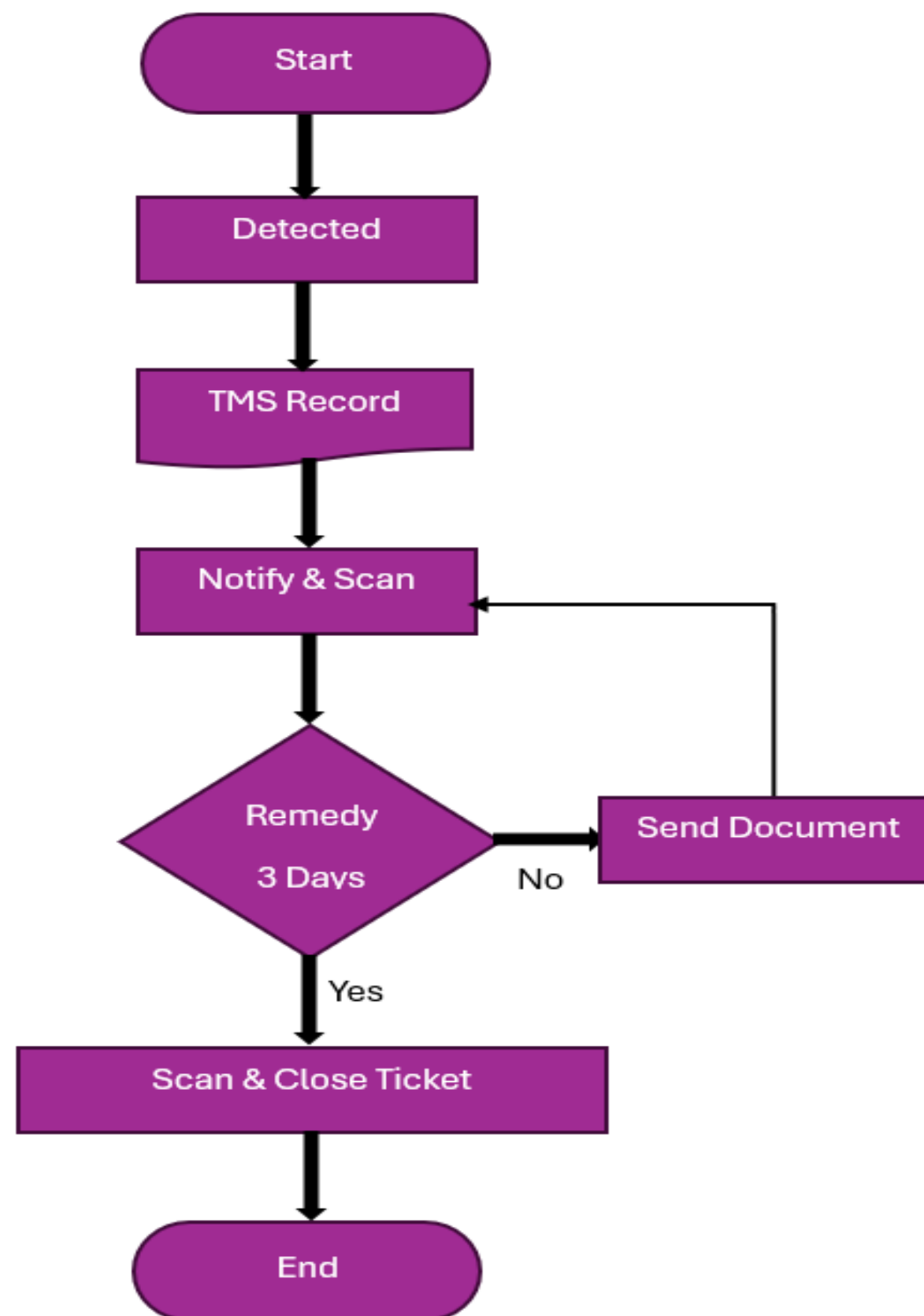
- ดำเนินการตาม พรบ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- ดำเนินการตาม ประกาศมหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567
- กระบวนการรับมือภัยคุกคามทางไซเบอร์
 - Preparation Detection Containment Post-Incident
- บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

ผลกระทบที่เป็นประโยชน์

- ขั้นตอนการปฏิบัติชัดเจนมีมาตรฐาน
- ลดการสูญเสียชื่อเสียง เพิ่มความมั่นใจ
- พัฒนาและเพิ่มคุณค่าบุคลากร



แผนการดำเนินงาน





Detected

- Google Search Engine



ทั้งหมด รูปภาพ วิดีโอ ข่าวสาร ข้อปั้ง เว็บ หนังสือ : เพิ่มเติม เครื่องมือ

 Chiang Mai University
https://rcsd.soc.cmu.ac.th › uploads › 2022/03 PDF :

GAMBLING AS DEVELOPMENT:

Rarely are Burmese **gamblers** seen playing **baccarat**, but they are more often found in the relatively small gaming centres, **gambling** on slot machines or dar yu ji ...

100 หน้า

 สำนัก บริการ วิชาการ
https://uniserv.cmu.ac.th › training :

เว็บพนันบอลดีที่สุด เว็บบอลราคาน้ำดีสุด บริการ 24 ชม.

เพราะเป็นผู้ให้บริการเดียว ที่สามารถสร้างความมั่นใจในเรื่องของการรวมเกม สล็อตเว็บตรง ที่ดีที่สุด แดกรางวัลได้จริง ไม่มีการล็อค User ทำให้คุณชนะเดิมพันแล้วรับเงินได้ทันทีอย่างมั่นใจ ไม่ต้องรอลานาน ...

 Chiang Mai University
https://e-meeting.eqd.cmu.ac.th › search :

บาคาร่าเว็บตรง คาสีโนออนไลน์ Online Casino – เล่นรับเงินจริง โบนัส 8

...

ดู บา ส สด ซีเกมส์ คาสีโนออนไลน์77คาสีโนออนไลน์เกมออนไลน์ · เว ป หวย · วิเคราะห์ บอล เต็ง คิน นี้ · สล็อต ยืนยัน otp รับเครดิตฟรี 50 ...

 AMS CMU
https://www.ams.cmu.ac.th › main › casino › juth=pretty... :

PRETTY BACCARAT 88 \$ มาปั่นสล็อตที่ ...



Detected

- EduShield

10:00

< 99+ LINE Notify

gambling2:
ระบบเฝ้าระวังภัยคุกคามการศึกษา
(EduShield)
สรุปผลการตรวจสอบเว็บไซต์:
มหาวิทยาลัยเชียงใหม่
โดเมน: cmu.ac.th
ถูกฝังโฆษณาพนัน: 1 ลิงก์
ถูกเปลี่ยนเส้นทาง: 0 ลิงก์
รวมทั้งหมด: 1 ลิงก์ที่ต้องตรวจสอบ
ศึกษารายละเอียดเพิ่มเติมได้ที่ :
<https://edushield.rmutl.ac.th/>

มหาวิทยาลัยเชียงใหม่ : Chiang Mai...
Chiang Mai University is University of
Excellence Where Nature Nurtures B...

Login
EduShield ระบบเฝ้าระวังภัยคุกคามการ
ศึกษา อย่าให้ภัยคุกคามทางไซเบอร์ แอบ...

08:55

EduShield | ระบบเฝ้าระวังภัยคุกคามการศึกษา

สวัสดี คุณโอกาส หมื่นแสน

หน่วยงาน : มหาวิทยาลัยเชียงใหม่

ภาพรวม ข้อมูลสถิติ ออกจากระบบ

รายงานการค้นพบข้อมูลเว็บพนัน : cmu.ac.th (อัปเดตเมื่อ 2024-09-25 09:02:12)

จำนวนเว็บพนันที่ยังตรวจสอบพบ	จำนวนเว็บพนันที่แก้ไขแล้ว
0	6

-- ทั้งหมด --

ข้อมูลพนันที่ยังคงพบในปัจจุบัน	วัน - เวลาที่ตรวจพบ
ไม่มีข้อมูล	

⚠ คำแนะนำเมื่อเกิดเหตุ



- Ticket Management System





Collect Evidence & Analysis

- Burp Suite

Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions Manually generated Search 🔍 ⋮								
Time	Source	Issue type ▾	Host	Path	Insertion point	Severity	Confidence	Comment
11:04:15 30 Oct 2024	Task 3	! XPath injection	https://finance.oou.cmu.ac.th	/cron.php	form_id parameter	High	Firm	
10:15:22 30 Oct 2024	Task 3	! XPath injection	https://finance.oou.cmu.ac.th	/demoweb/	q parameter	High	Firm	
10:05:52 30 Oct 2024	Task 3	! XPath injection	https://finance.oou.cmu.ac.th	/	q parameter	High	Firm	
10:20:58 30 Oct 2024	Task 3	? XML injection	https://finance.oou.cmu.ac.th	/	q parameter	Medium	Tentative	
10:01:01 30 Oct 2024	Task 3	? Vulnerable JavaScript dependency	https://finance.oou.cmu.ac.th	/sites/all/modules/jquery_update/replace/ui/ui.mi...		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	? Vulnerable JavaScript dependency	https://finance.oou.cmu.ac.th	/sites/all/modules/jquery_update/replace/ui/ui.mi...		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	? Vulnerable JavaScript dependency	https://finance.oou.cmu.ac.th	/sites/all/modules/jquery_update/replace/ui/ui.mi...		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	? Vulnerable JavaScript dependency	https://finance.oou.cmu.ac.th	/misc/jquery.js		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	? Vulnerable JavaScript dependency	https://finance.oou.cmu.ac.th	/sites/all/modules/jquery_update/replace/ui/ui.mi...		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	? Vulnerable JavaScript dependency	https://finance.oou.cmu.ac.th	/sites/all/modules/jquery_update/replace/ui/ui.mi...		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	? Vulnerable JavaScript dependency	https://finance.oou.cmu.ac.th	/		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	! TLS cookie without secure flag set	https://finance.oou.cmu.ac.th	/		Medium	Firm	
10:00:58 30 Oct 2024	Task 3	i TLS certificate	https://finance.oou.cmu.ac.th	/		Information	Certain	



ກຣະບວນກາຣ

- Notify
- Remedy 3 Days
- Send Document
- Close Ticket





วิเคราะห์และสรุปสาระสำคัญ

- ภัยไซเบอร์หลากหลาย รุนแรง ป้องกันไม่หมด
- มาตรฐานกระบวนการรับมือภัยคุกคามไซเบอร์
- ลดผลกระทบและความเสียหาย
- ปัญหา Web Defacement เว็บพ่น
- กระบวนการรับมือฯ ป้องกันความเสียหาย ชื่อเสียงมหาวิทยาลัย เพิ่มความมั่นใจ



THANK YOU