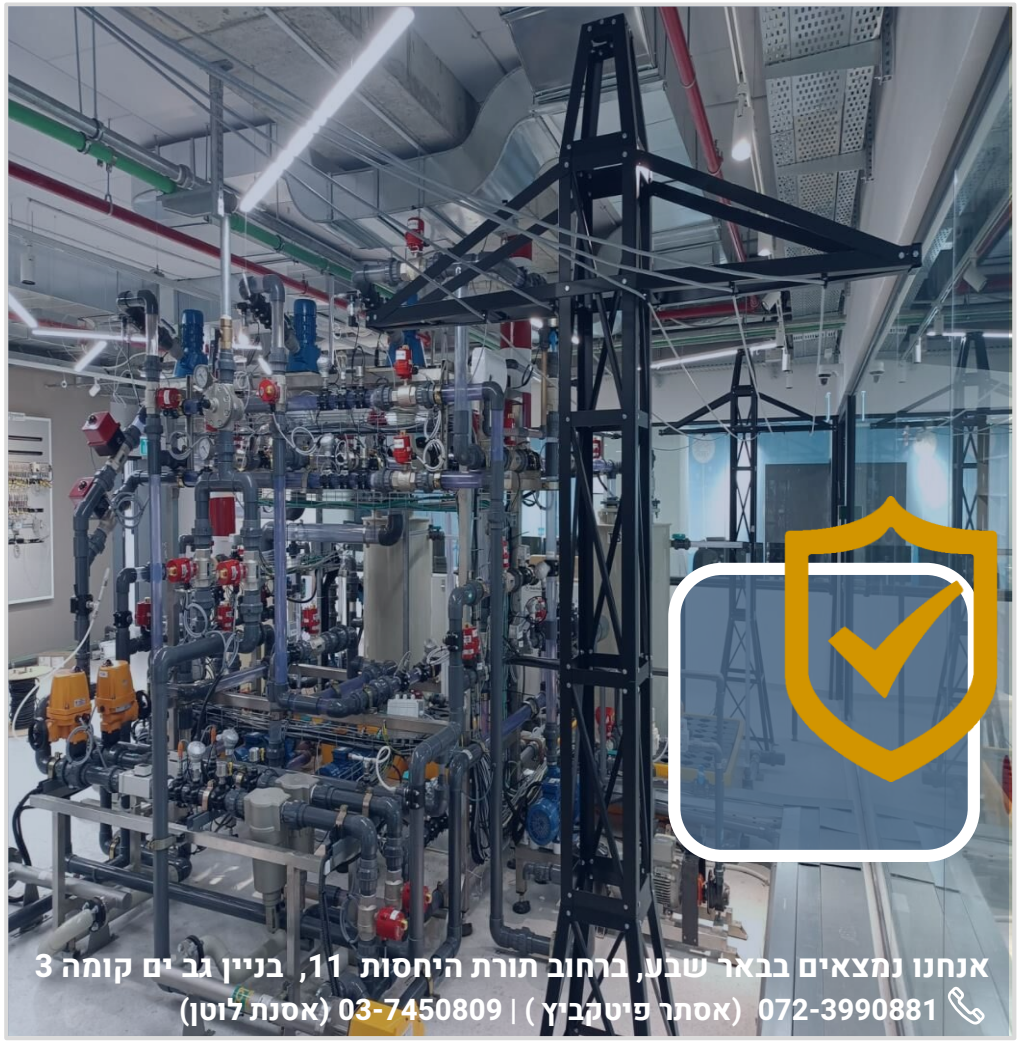
מעבדה לאומית לאנרגיה, בקרה וסייבר

תמונת מצב
מרכז מודיעין ICS

דוח מס. 2 – 08/06/2023



משרד האנרגיה
www.energy.gov.il

סייבר ישראל
Cyber Israel

המעבדה הלאומית
לאנרגיה, בקרה וסייבר

תמונת מצב – מרכז מודיעין ICS

עדכון זה מכיל עדכונים בתחום הסייבר הרלוונטיים למגזר האנרגיה, הבקרה והתשתיות ממקורות גלויים מגוונים

נושאים חמים

מרכז ידע עם גישה מהירה ונוחה לסוגי מידע שונים הקשורים להגנת סייבר – מחקרים, דוחות, סיכומים, דפי מידע של החברות המפתחות פתרונות להגנת סייבר, הדרכות, סטטיסטיקה ומאגרי מידע. פורטל של קבוצת קספרסקי.
https://start.me/p/wMrA5z/cyber-threat-intelligence?s=04

איום סייבר איראני - מחקרים מעמיקים על ההתפתחות של איום הסייבר של איראן – כולל היסטוריה, סיבות פוליטיות וכלכליות, שחקנים עיקריים בפעילות הזו, מצב נוכחי, סוגי פעילות, מטרות, מגמות ותחזיות
Iran Cyber Threat Overview - Sekoia.io Blog

Microsoft Security Compliance and Identity

תקני עבודה בתחום הגנת סייבר בתעשייה - עקרונות ודרישות של תקן בינלאומי ISO 27001:2022 לניהול הגנת סייבר באמצעות ISMS, דרישות המבחן CISSP לקבלת תעודה מבוססת על התקן הזה
https://medium.com/codex/the-essential-guide-to-iso-27001-2022-97adad7355c2

תמונת מצב – מרכז מודיעין ICS

עדכון זה מכיל עדכונים בתחום הסייבר הרלוונטיים למגזר האנרגיה, הבקרה והתשתיות ממקורות גלויים מגוונים

המלצות / טיפים

הגדרת סיסמה בטוחה וניהול סיסמאות, אבטחת מידע וגישה מאובטחת לנתונים

https://evotec-xyz.cdn.ampproject.org/c/s/evotec.xyz/strengthening-password-security-in-active-directory-a-powershell-powered-approach/amp/

https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy

https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/personal-data-encryption/

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#identifying-ipv6-traffic-with-azure-ad-sign-in-activity-reports

https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/conditional-access-authentication-strength-is-now-generally/ba-p/3773134

מאגרי מידע, גישה לכלים, מקורות ידע, ספריות מקצועיות והדרכות בנושא הגנת סייבר

https://gitlab.com/syntax-ir/playbooks

https://github.com/corazawaf/coraza

https://github.com/xalgord/Massive-Web-Application-Penetration-Testing-Bug-Bounty-Notes

תמונת מצב – מרכז מודיעין ICS

עדכון זה מכיל עדכונים בתחום הסייבר הרלוונטיים למגזר האנרגיה, הבקרה והתשתיות ממקורות גלויים מגוונים

המלצות / טיפים

עקרונות הפעילות, שיטות התקיפה ואפשרויות הגנה למכשירים מחוברים ב-Bluetooth

https://www.makeuseof.com/understanding-bluetooth-security/

אוסף כתבות על המגמות בעולם טכנולוגיות תקשורת

https://www.bynet.co.il/ictrends/?utm_campaign=top_strip_banner_on_ictrends_newsletter&utm_medium=ictrends_newsletter&utm_source=ictrends_04.2021

פגיעות והגנה של כלי Google מול תקיפות סייבר

https://cybersecuritynews.com/google-drive-security-flaw/

https://www.scmagazine.com/news/email-security/gmail-spoofing-google-priority-1-probe

תמונת מצב – מרכז מודיעין ICS

עדכון זה מכיל עדכונים בתחום הסייבר הרלוונטיים למגזר האנרגיה, הבקרה והתשתיות ממקורות גלויים מגוונים

מוצרים, שיטות וחברות בתחום ICS/OT

כלי להגנת סייבר למערכות ICS

https://www.msspalert.com/cybersecurity-services-and-products/honeywell-releases-operational-technology-solution-for-industrial-control-systems/

אינטליגנציה מלאכותית בהגנת סייבר

https://www.crowdstrike.com/blog/crowdstrike-introduces-charlotte-ai-to-deliver-generative-ai-powered-cybersecurity/

Microsoft Defender Threat Intelligence

https://jeffreyappel-nl.cdn.ampproject.org/c/s/jeffreyappel.nl/defender-ti-integrations-with-microsoft-sentinel/amp/

https://jeffreyappel.nl/how-works-microsoft-defender-threat-intelligence-defender-ti-and-what-is-the-difference-between-free-and-paid/

תמונת מצב – מרכז מודיעין ICS

עדכון זה מכיל עדכונים בתחום הסייבר הרלוונטיים למגזר האנרגיה, הבקרה והתשתיות ממקורות גלויים מגוונים

מחקרים ודוחות

מלחמת סייבר

https://cyberscoop.com/moonlighter-hack-a-sat-defcon/

https://www.neowin.net/news/crowdstrike-details-spyboy-terminator-said-to-kill-microsoft-defender-avast-and-more-edrs/

מהות תפקיד CISO במציאות החדשה

https://www.sdxcentral.com/articles/analysis/the-great-ciso-resignation-why-security-leaders-are-quitting-in-droves/2023/05/

פגיעות בשיטת זיהוי OAuth

https://salt.security/blog/a-new-oauth-vulnerability-that-may-impact-hundreds-of-online-services