

فهرست مطالب

پیش‌گفتار.....	۹
مقدمه.....	۱۰
چرا این کتاب را نوشتیم؟.....	۱۰
کتاب حاضر برای چه کسانی نوشته شده است؟.....	۱۱
ساختار کتاب.....	۱۲
راهنمای استفاده از کتاب.....	۱۳
فصل ۱ مبانی و چشم‌انداز تهدیدات سایبری در زیرساخت‌های حیاتی.....	۱۴
۱-۱- مقدمه.....	۱۴
۱-۲- تعاریف و مفاهیم پایه.....	۱۴
چالش همگرایی OT/IT و شکست راهبرد شکاف هوا.....	۱۵
۱-۳- چشم‌انداز تهدیدات سایبری (تحلیل سال‌های ۲۰۲۵ و ۲۰۲۶).....	۱۶
۱-۳-۱- نقش گروه‌های APT (تهدیدات پیشرفته و پایدار).....	۱۶
۱-۳-۲- تکامل حملات باج‌افزاری (Ransomware) در بخش OT.....	۱۷
۱-۳-۳- به‌کارگیری هوش مصنوعی در حملات سایبری.....	۱۷
۱-۳-۴- حملات زنجیره تأمین (Supply Chain Attacks).....	۱۷
۱-۴- صنعت آب و فاضلاب: چالش‌ها و ویژگی‌های پدافندی.....	۱۸
نمونه واقعی: بدافزار FrostyGoop و درس‌های آن برای صنعت آب.....	۱۸
نمونه واقعی: حادثه تصفیه‌خانه اولدزمار در آمریکا.....	۱۹
بررسی آسیب‌پذیری‌های ساختاری در تصفیه‌خانه‌ها.....	۱۹
۱-۵- خلاصه و جمع‌بندی فصل.....	۲۰
مراجع فصل ۱ (References).....	۲۱
فصل ۲ تهدیدات خاص (بدافزارها، باج‌افزارها و گروه‌های APT).....	۲۲

۲۲	۱-۲- مقدمه
۲۳	۲-۲- باج‌افزارها (Ransomware): تهدید غالب و در حال رشد
۲۴	۳-۲- بدافزارهای صنعتی (Industrial Malware): سلاح‌های دیجیتال دقیق
۲۵	۴-۲- فعالیت گروه‌های APT و تهدیدات تحت حمایت دولت‌ها
۲۶	۵-۲- خلاصه و جمع‌بندی
۲۷	مراجع فصل ۲ (References)
۲۸	فصل ۳ همگرایی OT/IT و گسترش سطح حمله (Attack Surface)
۲۸	۱-۳- مقدمه
۲۹	۲-۳- مزایا و مخاطرات همگرایی OT/IT
۳۰	۳-۳- آسیب‌پذیری سیستم‌های OT در برابر نفوذ از طریق لایه IT
۳۱	۴-۳- مهم‌ترین عوامل گسترش سطح حمله در تصفیه‌خانه‌ها
۳۲	۵-۳- راهکارهای راهبردی کاهش سطح حمله
۳۳	۶-۳- خلاصه و جمع‌بندی
۳۴	مراجع فصل ۳ (References)
۳۵	فصل ۴ استانداردها و چارچوب‌های حاکمیت امنیت (NIST CSF 2.0)
۳۵	۱-۴- مقدمه
۳۶	۲-۴- چارچوب NIST CSF 2.0 چیست و چرا اهمیت دارد؟
۳۷	۳-۴- سه جزء اصلی چارچوب NIST CSF 2.0
۳۷	۱-۳-۴- هسته مرکزی: شش کارکرد اصلی
۳۸	۲-۳-۴- سطوح پیاده‌سازی (Implementation Tiers)
۳۹	۳-۳-۴- نمایه (Profile)
۳۹	۴-۴- تابع Govern (حکمرانی): قلب تپنده CSF 2.0

۴-۵- هم‌ترازی چارچوب با استانداردهای نوین (مدل‌های ۲۰۲۵ و ۲۰۲۶).....	۴۰
۴-۶- گام‌های عملی برای پیاده‌سازی (مطالعه موردی فرضی).....	۴۰
۴-۷- خلاصه و جمع‌بندی.....	۴۲
مراجع فصل ۴ (References).....	۴۲
فصل ۵ هوش مصنوعی (AI)؛ شمشیر دو لبه در امنیت زیرساخت‌های حیاتی.....	۴۳
۵-۱- مقدمه.....	۴۳
۵-۲- هوش مصنوعی به عنوان یک «نیروی چندبرابرکننده» برای مهاجمان.....	۴۴
۵-۲-۱- تسریع و خودکارسازی چرخه حمله.....	۴۴
۵-۲-۲- خودکارسازی کامل عملیات توسط عوامل هوشمند (Agentic AI).....	۴۵
۵-۳- آسیب‌پذیری‌های خودِ هوش مصنوعی (حمله به مدل‌های AI).....	۴۶
۵-۴- هوش مصنوعی به عنوان ابزاری برای مدافعان.....	۴۷
۵-۵- حاکمیت امنیت و چارچوب‌های مرتبط با هوش مصنوعی.....	۴۸
۵-۶- چشم‌انداز آینده: همکاری انسان و ماشین.....	۴۹
۵-۷- خلاصه و جمع‌بندی.....	۴۹
مراجع فصل ۵ (References).....	۵۰
فصل ۶ پدافند سایبری و تاب‌آوری (آمادگی برای بحران).....	۵۱
۶-۱- مقدمه.....	۵۱
۶-۲- از امنیت تا تاب‌آوری؛ تغییر پارادایم و نگاه استراتژیک.....	۵۲
۶-۳- متدولوژی ارزیابی تاب‌آوری در تصفیه‌خانه؛ گام نخست.....	۵۳
۶-۴- مؤلفه‌های کلیدی یک برنامه تاب‌آوری جامع.....	۵۴
۶-۵- هشدارها و چالش‌های پدافندی.....	۵۵
۶-۶- خلاصه و جمع‌بندی.....	۵۵
مراجع فصل ۶ (References).....	۵۶

فصل ۷ امنیت زنجیره تأمین (Supply Chain Security) ۵۷

۷-۱- مقدمه ۵۷

۷-۲- تهدیدات زنجیره تأمین: مسیرهای اصلی نفوذ ۵۸

۱. نفوذ از طریق فروشندگان و پیمانکاران ۵۸

۲. آلودگی سخت‌افزاری ۵۸

۳. آلودگی نرم‌افزاری و به‌روزرسانی‌های جعلی ۵۹

۷-۳- ارزیابی و مدیریت ریسک فروشندگان ۵۹

گام اول: شناسایی و دسته‌بندی فروشندگان ۵۹

گام دوم: ارزیابی امنیتی فروشندگان ۵۹

گام سوم: پیاده‌سازی کنترل‌های دسترسی ۵۹

گام چهارم: نظارت و پایش مستمر ۶۰

۷-۴- اقدامات عملی برای مقابله با سخت‌افزار و نرم‌افزار آلوده ۶۰

راهکار اول: محیط قرنطینه سخت‌افزاری (Sandbox) ۶۰

راهکار دوم: احراز هویت و سنجش یکپارچگی نرم‌افزار ۶۰

راهکار سوم: سیاست به‌روزرسانی محافظه‌کارانه ۶۱

راهکار چهارم: مدیریت پیچ مبتنی بر اولویت‌بندی ۶۱

۷-۵- خلاصه و جمع‌بندی ۶۱

منابع و مراجع فصل ۷ ۶۲

فصل ۸ اقدامات عملی و اولویت‌بندی دفاعی (فهرست کارهای ضروری) ۶۳

۸-۱- مقدمه ۶۳

۸-۲- سطح اول: اقدامات فوری و کم‌هزینه (۰ تا ۳ ماه) ۶۳

تغییر رمزهای عبور پیش‌فرض و ضعیف: ۶۴

فعال‌سازی احراز هویت چندعاملی (MFA) برای دسترسی از راه دور: ۶۴

- ۶۴ غیرفعال کردن حساب‌های کاربری بی‌استفاده:
- ۶۴ برگزاری جلسه آگاه‌سازی برای کارکنان:
- ۶۵ ۸-۳- سطح دوم: اقدامات میان‌مدت (۳ تا ۱۲ ماه):
- ۶۵ پیاده‌سازی پشتیبان‌گیری منظم و آفلاین:
- ۶۵ تهیه و تمرین برنامه واکنش به حادثه (Incident Response Plan):
- ۶۵ مدیریت آسیب‌پذیری مبتنی بر ریسک:
- ۶۶ ۸-۴- سطح سوم: اقدامات بلندمدت و سرمایه‌ای (بیش از ۱۲ ماه):
- ۶۶ استقرار سیستم مانیتورینگ پیوسته برای شبکه OT:
- ۶۶ مهاجرت تدریجی به معماری «اعتماد صفر» (Zero Trust):
- ۶۶ ایجاد برنامه «تیم قرمز» داخلی:
- ۶۷ بازنگری و به‌روزرسانی دوره‌ای خط‌مشی‌ها و فرآیندها:
- ۶۷ ۸-۵- ابزارهای متن‌باز: جایگزینی برای شرایط تحریم:
- ۶۸ ۸-۶- جمع‌بندی و توصیه نهایی:
- ۶۹ منابع و مراجع فصل ۸:
- ۷۰ فصل ۹ آموزش و فرهنگ‌سازی کارکنان:
- ۷۰ ۹-۱- مقدمه:
- ۷۱ ۹-۲- اهمیت آموزش کارکنان به عنوان لایه‌ی دفاعی اصلی:
- ۷۱ ۹-۳- محتوای آموزشی متناسب با نقش کارکنان:
- ۷۲ سطح دوم: آموزش تخصصی برای اپراتورهای OT و کارشناسان فنی:
- ۷۳ سطح سوم: آموزش مدیریت ارشد (مدیر عامل، اعضای هیئت مدیره):
- ۷۳ ۹-۴- روش‌های اجرایی مؤثر برای آموزش مستمر:
- ۷۴ آموزش‌های کوتاه و مکرر (Micro-Learning):
- ۷۴ بازی‌سازی (Gamification):

تمرین‌های رومیزی (Tabletop Exercises).....	۷۴
بازخورد و جوایز:.....	۷۴
۹-۵- چالش‌های پیاده‌سازی و راهکارها.....	۷۵
۹-۶- خلاصه و جمع‌بندی.....	۷۵
منابع و مراجع فصل ۹.....	۷۶
فصل ۱۰ چشم‌انداز آینده و فناوری‌های نوظهور.....	۷۷
۱۰-۱- مقدمه.....	۷۷
۱۰-۲- روند نخست: رایانش کوانتومی و پایان رمزنگاری کلاسیک.....	۷۷
برای یک تصفیه‌خانه، اقدامات زیر توصیه می‌شود:.....	۷۸
۱۰-۳- روند دوم: بلوغ عامل‌های هوشمند و نیاز به حاکمیت جدید.....	۷۸
۱۰-۴- روند سوم: امنیت زیرساخت‌های فضایی (ماهواره‌ها).....	۷۹
برای صنعت آب ایران:.....	۷۹
۱۰-۵- روند چهارم: ژئوپلیتیک تحریم‌ها و زنجیره تأمین سخت‌افزاری.....	۷۹
۱۰-۶- روند پنجم: تثبیت استانداردهای صنعتی (IEC 62443).....	۸۰
برای صنعت آب ایران:.....	۸۰
۱۰-۷- روند ششم: تحول در آموزش با کمک هوش مصنوعی.....	۸۱
۱۰-۸- جمع‌بندی و نقشه‌راه پیشنهادی برای دهه آینده.....	۸۱
مرحله اول (اکنون تا ۲۰۲۸) -- آماده‌سازی:.....	۸۱
مرحله دوم (۲۰۲۸ تا ۲۰۳۲) -- مهاجرت و انطباق:.....	۸۱
مرحله سوم (۲۰۳۲ به بعد) -- بلوغ و بهینه‌سازی:.....	۸۲
منابع و مراجع فصل ۱۰.....	۸۳
واژه‌نامه (Glossary).....	۸۴