مدبران

ارایه راهکارهای امنیت سیستمهای کنترل صنعتی

www.modaberan-ics.com

START | شروع

Smart Catalog

مدبران

ارایه راهکارهای امنیت سیستمهای کنترل صنعتی

www.modaberan-ics.com

Secure IoT Gateway

Unidirectional Gateway

Data Diode

سیستم مدیریت دارایی شبکه صنعتی

مشاوره امنیت صنعتی

SIEM صنعتی

تست نفوذ صنعتی

آموزش امنیت صنعتی

ساخت و تولید

Secure IoT Gateway

Secure IoT Gateway یک دستگاه فیزیکی و برنامه نرم‌افزاری است که به عنوان نقطه اتصال بین کنسول مرکزی و کنترل کننده‌ها، حسگرها و دستگاه‌های هوشمند عمل می‌کند. همه داده‌هایی که بین دستگاه‌های اینترنت اشیا و نقطه مرکزی در حال حرکت هستند از یک دروازه اینترنت اشیا عبور می‌کنند که می‌تواند یک ابزار سخت افزاری اختصاصی یا یک برنامه نرم‌افزاری باشد.

CYRUS Secure IoT gateway یک منبع واحد از داده‌های صنعتی را برای همه دستگاه‌های اتوماسیون، ماشین آلات و نرم افزارهای کاربردی فراهم می‌کند. CYRUS ضمن تامین امنیت مورد انتظار، با بیش از ۵۰ درایور و افزونه‌های پیشرفته، انعطاف‌پذیری لازم برای غلبه بر هر گونه چالش اتصال داده در شبکه‌های IoT را دارد.

فایروال صنعتی Tofino

Unidirectional Gateway

یکسو کننده ارتباطات صنعتی در لایه سرویس، مناسب برای نصب میان Zoneهای شبکه صنعتی

به دلیل گسترش سیستم‌های اطلاعاتی و نرم‌افزارهای مدیریتی در سازمان‌ها و کارخانه‌ها غالبا لازم می‌شود که یک سری اطلاعات از شبکه صنعتی به شبکه اداری انتقال داده شود. اما به دلایل امنیتی لازم است انتقال این اطلاعات به روشی امن و یک طرفه برقرار شود تا از ورود تهدیدات احتمالی موجود در شبکه اداری به صنعتی جلوگیری شود.

محصول Unidirectional Gateway این ارتباط را یک طرفه کرده و یک طرفه بودن ارتباط بین دو شبکه را بصورت سخت افزاری گارانتی می کند بگونه‌ای که هرگونه اشتباه اپراتور در تنظیمات این محصول نمی‌تواند منجر به برقراری ارتباط دوطرفه شود.

ویژگی ها و مزایا

- سخت افزار کاملا ماژولار و قابل انعطاف با ویژگی‌های امنیتی بالا و سازگار با محیط‌های صنعتی
- توان انتقال 1Gbps ، امکان اضافه کردن پهنای در مدلهای بالاتر
- باند با چندین جفت TX / RX

- دارای سرویس پشتیبان HA (اختیاری)
- تمامی اتصالات جلوی دستگاه تعبیه شده تا بصورت واضح دیده شده و بتوان بر روی آنها کار کرد
- طیف گسترده‌ای از اتصال دهنده‌های نرم افزاری، بدون نیاز به هزینه سفارشی‌سازی
- شناسایی بیش از ۱۵۰ نوع پروتکل
- انتقال یکسویه داده‌ها از یک Network به Network دیگر
- شبیه‌سازی پروتکل‌ها در سمت شبکه IT
- امکان لاگ‌گیری از داده‌ها در دوطرف
- امکان اتصال داده‌ها به سیستم Splunk و تعیین Threshold برای هر تگ
- امکان Schedule کردن اتصال به سیستم صنعتی و لاگ‌گیری
- امکان ایجاد آلارم و Event بر اساس تگ‌ها و ارسال آن به سرورهای آلارم و Event
- امکان محاسبات پیچیده از روی تگ و ساخت یک تگ جدید

Data Diode

دیتا دیود یک ابزار سخت‌افزاری برای یک سویه کردن ارتباط میان دو نقطه در شبکه است. در شبکه‌های حساس صنعتی گاهی لازم می‌شود که ارتباط میان دو شبکه یک سویه شود. دیتادیود سایروس به شما این امکان را می‌دهد که ارتباط میان دو نقطه را یک طرفه کنید. یک سویه شدن ارتباط بصورت سخت‌افزاری گارانتی می‌شود.

در صورت استفاده از دیتادیود روی خط، به هیچ وجه نمی‌شود ارتباط دوطرفه میان دوشبکه برقرار کرد. شرکت مدبران با تولید اختصاصی دیتادیود، نیاز به این محصول را در کشور برطرف کرده است. ذکر این نکته لازم است که محصول Unidirectional Gateway محصول تکامل یافته تری نسبت به دیتادیود است.

فایروال صنعتی Moxa

سیستم مدیریت دارایی شبکه صنعتی

مدیریت دارایی در شبکه‌های صنعتی یک موضوع پایه‌ای و حساس است و در مدیریت صحیح حوادث و مشکلات نقشی کلیدی دارد. مدیریت دارایی یک ابزار مهم تصمیم‌گیری در مورد سخت‌افزارها و نرم افزارهای IT/OT محسوب می‌شود.

بدون داشتن یک سیستم مناسب مدیریت دارایی در شبکه صنعتی نمی توان به نتیجه مطلوب در ارتقای امنیت یک واحد صنعتی دست پیدا کرد.

شرکت مدبران با بکارگیری ابزارهای متنوع، سیستم مدیریت دارایی در شبکه صنعتی را به مشتریان خود ارائه می کند که به کمک آن می توان مشخصات سخت افزاری و نرم افزاری سیستم ها را تعریف و ارتباط آنها را مورد بررسی قرار داد و همچنین مشکلات ایجاد شده روی هر سیستم و یا PLC و هر Asset دیگر را با درخواست کاربران، مدیریت کرد و با ارجاع به تکنسین مربوطه به مشکلات آن ها رسیدگی کرد.

یک مجموعه صنعتی با داشتن سیستم مدیریت دارایی صنعتی شرکت مدبران از مزایای زیر برخوردار خواهد شد:

- صرفه جویی در هزینه
- کاهش خطر
- افزایش کارآیی و اثربخشی
- پایداری

- امکان مدیریت درخواست ها، رخدادها و حوادث
- مدیریت مشکلات
- مدیریت تغییرات
- مدیریت خدمات
- تعریف دارایی یا Assets های سازمان
- گزارش‌گیری آسان و راحت

این گزارشات می تواند مواردی مانند:

- تهیه گزارش از تمام قراردادها و پروژه ها
- تهیه لیستی از نرم افزارهای نصب شده بر روی سیستم ها با جزئیات
- تهیه گزارشی از تمام درخواست ها و یا سفارشات
- تهیه گزارشاتی از مشکلات موجود در یک بازده زمانی
- تهیه لیستی از Firmwareهای نصب شده بر روی PLCها
- تهیه دارایی ها و یا اموال سازمان و یا اداره خود با تمام جزئیات
- تهیه لیستی از تمام خریدها
- و ... باشد.

مشاوره امنیت صنعتی

متاسفانه ایران همواره در کانون حملات سایبری بویژه حملات سایبری صنعتی قرار داشته است. لذا ارتقای سطح امنیت شبکه‌های صنعتی بویژه سیستم‌های کنترل از اهمیت بسیار بالایی در کشور برخوردار است.

شرکت مدبران با بیش از ۱۲ سال تجربه در حوزه امنیت سیستم‌های کنترل صنعتی و با بهره‌گیری از کارشناسان مجرب، آمادگی ارائه خدمات مشاوره‌ای زیر را به زیر ساختهای حیاتی و صنایع کشور شامل نیروگاه، توزیع برق، مدیریت برق، نفت، ایستگاه‌های تقویت فشار گاز، پتروشیمی، فولاد و سایر صنایع مجهز به سیستم کنترل (شبکه DCS و اسکادا) دارد:

- مشاوره در امن‌سازی زیرساخت‌ها و سیستم‌های کنترل صنعتی
- بررسی نقشه‌ها و معماری سیستم کنترل صنعتی فعلی و ارتباطات موجود در آنها و ارائه مشاوره جهت اصلاح معماری مطابق با استانداردهای امنیتی
- مشاوره در انتخاب محصولات امنیتی در حوزه صنعتی
- مشاوره در نحوه بکارگیری محصولات امنیتی صنعتی
- مشاوره در تحلیل رخدادهای امنیت صنعتی
- مشاوره در انتخاب پروتکلهای صنعتی
- مشاوره در تبادل اطلاعات میان بخشهای مختلف صنعتی
- مشاوره در خصوص راه‌اندازی مراکز SOC صنعتی
- مشاوره در خصوص تجمیع سیستم‌های نظارتی در شبکه‌های صنعتی
- مشاوره تست نفوذ صنعتی

- مشاوره در تشخیص نابهنجاری در شبکه صنعتی
- مشاوره در خصوص راه اندازی آزمایشگاه‌های امنیت صنعتی
- مشاوره در خصوص ساخت و تولید تجهیزات سفارشی سخت افزاری مورد نیاز در حوزه امنیت صنعتی
- مشاوره در خصوص برگزاری دوره های آموزشی امنیت صنعتی و تربیت کارشناسان امنیت صنعتی

SIEM صنعتی

امروزه استفاده از نرم‌افزارهای SIEM در شبکه‌های سازمانی رایج شده است. هدف از SIEM شناسایی و طبقه‌بندی حوادث و وقایع و دسته‌بندی آنها و سپس تجزیه و تحلیل رخدادها جهت شناسایی و واکنش به مخاطرات است.

پیاده‌سازی SIEM صنعتی گرچه شباهت‌هایی با SIEMهای اداری دارد اما تفاوتهای اساسی هم میان آنها وجود دارد.

امروزه استفاده از شبکه‌های اسکادا و ICS گسترش زیادی پیدا کرده است و این شبکه‌ها روی بسترهای اینترنت و اینترانت مورد استفاده گسترده قرار می‌گیرند. شبکه‌های توزیع برق مثال خوبی از استفاده از شبکه‌های اسکادا در سطح گسترده با ارتباطات متنوع هستند.

تجزیه و تحلیل رخدادهای موجود در شبکه‌های اسکادا مستلزم پیاده‌سازی صحیح SIEM صنعتی است. SIEM صنعتی با دریافت Logها و Eventها مختلف از تجهیزات مختلف صنعتی شامل PLCها، IDSهای صنعتی، فایروالهای صنعتی، RTUها، سنسورها و سایر تجهیزات موجود در شبکه اسکادا و سپس تجزیه و تحلیل رخدادها امکان نمایش تهدیدات و نابهنجاری‌های صنعتی را فراهم می آورد.

پیاده‌سازی صحیح یک SIEM صنعتی در یک صنعت مستلزم شناخت و تحلیل دقیق از فرایندهای یک شبکه اسکادا یا ICS است. شرکت مدبران با در اختیار داشتن یک تیم مجرب، امکان پیاده‌سازی حرفه‌ای SIEM صنعتی در صنایع مختلف را فراهم آورده است.

تست نفوذ صنعتی

تست نفوذ صنعتی به معنای شناسایی آسیب پذیری‌های موجود در یک شبکه صنعتی و اجرای Exploit مرتبط با آنها برای اثبات ناامنی شبکه صنعتی است. بدیهی است که اجرای عملیات تست نفوذ در محیط عملیاتی می‌تواند مخاطره آمیز باشد. لذا تست نفوذ صنعتی غالبا در یک محیط آزمایشگاهی شبیه‌سازی شده اجرا می‌شود.

شرکت مدبران با بهره‌گیری از کارشناسان مجرب تست و نفوذ صنعتی امکان ارائه این خدمات را برای صنایع مختلف دارد.

تولید Malware های صنعتی

تیم تست و نفوذ صنعتی شرکت مدبران به استفاده از ابزارهای رایج تست و نفوذ صنعتی اکتفا نکرده و برای پروژه‌های خود بصورت اختصاصی اقدام به تولید Malwareهای صنعتی می کند. تولید Malwareهای اختصاصی این امتیاز را دارد که توجه به ساختار پیاده‌سازی شده در یک شبکه صنعتی به صورت اثربخش تری از آسیب پذیری‌های موجود استفاده کرده و وجود ناامنی را اثبات می‌کند.

شرکت مدبران در کنار اجرای پروژه‌های تست و نفوذ صنعتی اقدام به ارائه مشاوره به مشتریان خود جهت رفع آسیب پذیری‌های کشف شده می‌نماید. محدوده تست نفوذ صنعتی بسته به نوع شبکه اسکادا و ICS می‌تواند شامل موارد زیر باشد:

- Firmwareهای تجهیزات
- نرم افزارها
- شکستن رمزنگاری
- سخت افزار
- شبکه

آموزش امنیت صنعتی

شرکت مدبران مجری تخصصی ترین و کاربردی ترین دوره های آموزشی امنیت سیستم های کنترل صنعتی در کشور

دوره آموزشی Industrial Control Systems (ICS) Security (امنیت در سیستمهای کنترل صنعتی):

مخاطبان:

- مدیران و کارشناسان شبکه و امنیت اطلاعات سازمان
- مدیر فناوری اطلاعات
- مدیر و کارشناسان IT حراست
- مدیر و کارشناسان سیستم های کنترل صنعتی
- مدیر و کارشناسان برق و ابزار دقیق

سرفصل ها:

۱- معرفی ساختار و معماری سیستم های کنترل صنعتی و اسکادا

- فرایند ها و نقش ها
- کارخانجات
- فیلدها و کنترل ها
- کنترل های قابل برنامه ریزی
- HMIs, Historians, Alarm Servers
- Specialized Applications and Master Servers

- DCS and SCADA
- Secure ICS Network Architectures

۲- معرفی ساختار و معماری پروتکل ها و شبکه‌های صنعتی و ارائه روش‌هایی جهت انجام اصلاحات موردنیاز، برای ارتقای امنیت، بر اساس ساختار شبکه موجود

- Modbus
- SYComm
- SYCommPlus
- Profibus
- OPCUA

۳- امنیت در سیستم‌های کنترل صنعتی و اسکادا

- بازیگران تهدید و دلایل حمله
- تاکتیک‌ها و تکنیک‌های حمله بر اساس فریمور MITRE ATTACK و معرفی حملات Zero-Day
- روش مدیریت دارایی در صنعت
- روش‌ها و کاربرد آنالیز ریسک (مدیریت ریسک و مهندسی ریسک) و شناسایی نقاط نفوذ در یک مجموعه صنعتی
- راه‌کارهای ایمن‌سازی سیستم‌های صنعتی و طراحی معماری امنیت صنعتی و نحوه چیدمان تجهیزات امنیت صنعتی
- تفاوت فایروال‌های صنعتی با دیگر فایروال‌ها و بیان دلیل الزام وجود یک فایروال صنعتی در شبکه صنعتی
- توضیح اجمالی در رابطه با SOC و SIEM صنعتی و چرخه حیات امنیت صنعتی

٤- بررسی راه‌های نفوذ به سیستم‌های کنترل صنعتی

- شبکه
- پورت سریال
- استخراج رمز عبور از داخل EEPROM
- نفوذ به سیستم وای فای

٥- معرفی انواع حملات سایبری به سیستم‌های کنترل صنعتی و اسکادا

- پروتکل
- Historians and Databases
- Bypassing Auth with SQL Injection
- HMI and UI Attacks
- Web-based Attacks
- Password Fuzzing
- Sniffing, DoS, Masquerading, Rogue AP

٦- روش‌های جلوگیری از حملات سایبری

- سیستم عامل
- TPM And Tamper
- پروتکل امن
- روش‌های ایمن‌سازی و بررسی نقاط آسیب پذیر در نرم افزار Wincc ٧
دیتابیس‌ها
- نحوه ایمن کردن PLCها سرورهای بکاپ‌گیری و بکاپ اطلاعات
- بررسی لیست سفید سیستم‌های صنعتی و بیان ضرورت ایجاد آن

- امنیت فیزیکی سرورها، سوییچ ها و سیستم های صنعتی
- معرفی قابلیت User Manager جهت تعیین دسترسی یوزرها به پروژه‌ها، جلوگیری از دانلود غیرمجاز کاربران و ...
- Firewalls and NextGen Firewalls
- Data Diodes and Unidirectional Gateways

۷- تشریح یک حمله سایبری به صورت کامل به زیرساخت های صنعتی

- Stuxnet

همچنین در این دوره چند سناریوی عملی حمله به یک Plant صنعتی مانند نیروگاه و یا پتروشیمی تشریح خواهد شد.

ساخت و تولید

تولید محصولات سخت افزاری صنعتی سفارشی

شرکت مدبران با تجهیز کارگاه های تخصصی طراحی و ساخت تجهیزات الکترونیکی و با جذب کارشناسان مجرب، خدمات طراحی محصول شامل طراحی کیس(Enclosure)، سخت افزار، سیستم عامل و نرم افزار را برای تولید سفارشی محصولات انجام می دهد.

خدمات طراحی و سفارشی سازی سخت

طراحی و سفارشی سازی سخت افزار در بیشتر پروژه های Embedded انجام می شود. در برخی از پروژه ها نیاز به طراحی یک بخش سخت افزاری مجزا می باشد و در برخی دیگر نیاز به اصلاح یک سخت افزار موجود و تغییر آن برای یک مسئله خاص دارند.

در شرکت مدبران خدمات طراحی های بسیار پیچیده چند لایه با فرکانس بالا و سفارشی سازی ساخت PCB های خاص انجام می شود.

تولید نرم افزارهای صنعتی سفارشی

صنایع مختلف شیوهٔ کار و نیازهای گوناگونی دارند. ممکن است نوع کسب و کار یک صنعت، به حدی منحصر به فرد یا پیچیده باشد که نرم افزار مناسبی برای پاسخ به نیازهای آن در بازار موجود نباشد و یا نرم افزار های موجود فقط بخشی از نیازهای مشتری را تامین کنند.

شرکت مدبران با تکیه بر توان مهندسین خود امکان اجرای پروژه های نرم افزاری سفارشی برای صنایع مختلف را دارد.

مدبران

ارایه راهکارهای امنیت سیستمهای کنترل صنعتی

www.modaberan-ics.com

دفتر تهران

پاسداران، گلستان ۵، نبش خیابان اسلامی، ساختمان آرسس، واحد ۴۰۴

دفتر کرج

جهانشهر، میدان شهید مدنی، ساختمان آفتاب، واحد ۳

شماره فراگیر : ۰۲۱۹۱۰۰۵۶۶۷

پست الکترونیک : info@modaberan-ics.com

وب سایت : www.modaberan-ics.com