۱- رزومه اسماعیل باقری اصل

بنده با طبقه‌بندی فعالیت‌های خود، دسته‌بندی‌هایی را ایجاد نمودم که بتوانم مسیر طی شده توسط اینجانب را توصیف کنم.

۱-۱- مشخصات فردی

- نام : اسماعیل
- نام خانوادگی : باقری اصل
- مدرک تحصیلی : کارشناسی کامپیوتر – گرایش سخت افزار و دانشجوی کارشناسی ارشد رشته مدیریت فناوری اطلاعات
- تاریخ تولد : ۱۳۶۲/۶/۲۷
- محل تولد : تهران
- دین: اسلام، شیعه
- ملیت : ایرانی
- وضعیت تاهل : متاهل
- شماره همراه : ۰۹۱۲۵۰۶۵۱۹۷

Email: i@ICSdefender.ir

۱-۲- مشاغل و فعالیت‌ها

۱-۲-۱- مشاور دادگاه جرایم رایانه‌ای از سال ۸۷ الی ۸۹

بنده در این مقطع به عنوان مشاور در امور سیستم‌ها مشغول به فعالیت شدم که با توجه به درک مباحث امنیت بصورت خودآموز توانستم در چندین پرونده مشاوره لازم را به قضات بدهم.

۱-۲-۲- شرکت تک‌نت از سال ۸۹ الی ۹۰:

شرکت تک‌نت یکی از فراهم کنندگان اینترنت و پهنای باند بدون سیم و شبکه MPLS و همچنین به عنوان رابط انتقال داده صوتی از کشورهای همسایه به داخل کشور بود. بنده

آخرین سمت: مدیر NOC

۱-۲-۳- مرکز امنیت فناوری اطلاعات حفیظ ۹۰ ای ۹۵

مرکز امنیت فناوری اطلاعات حفیظ که با ماموریت تست‌نفوذ زیرساخت‌های حساس و حیاتی کشور در پایگاه جوادالائمه وابسته به قرارگاه میثاق ایجاد شده بود. بنده در سال ۹۰ موفق شدم به این مرکز بپیوندم. عمده فعالیت‌های این مرکز با توجه به نیازهای کشور و در برخی مواقع پروژه‌های سازمان پداند غیر عامل بوده است.

۱-۲-۴- شرکت امن‌افزار گستر شریف ۹۵ تا به اکنون

با توجه به نیاز این شرکت برای تولید SIEM صنعتی و ایجاد ساختار مرکز عملیات امنیت صنعتی به این شرکت پیوستم که تا به اکنون نیز در حال طراحی سنسورهای تشخیص نفوذ صنعتی و همچنین مرکز عملیات امنیت صنعتی می‌باشم.

۱-۲-۵- پژوهشکده پارسا شریف ۹۵ تا به اکنون

با توجه به احساس نیاز کشور به تولید محتوای بومی و همچنین نبود دانش کافی در زمینه امنیت زیرساخت‌های صنعتی بنده تصمیم گرفتم که با پژوهشکده در قالب نگارش کتاب آموزش امنیت سیستم‌های کنترل صنعتی و همچنین نگارش مقالات مرتبط با امنیت در زیرساخت‌های حساس و حیاتی همکاری داشته باشم.

۱-۲-۶- تاسیس مجموعه حفاظت کنندگان از زیرساخت‌های حساس و حیاتی شش ماهه دوم سال ۹۶ تا به اکنون(www.ICSdefender.ir)

با توجه به نبود امکان انتقال دانشم به علاقمندان در این حوزه و همچنین سایر مخاطبین عزیز و نیاز هرچه بیشتر به این دانش در کشور بنده تصمیم به تاسیس مجموعه **ICSdefender** گرفتم که بتوانم دانشم را بصورت رایگان در اختیار علاقمندان قرار دهم.

۱-۳- مدارک اخذ شده و دوره‌های گذرانده شده

با توجه به گستردگی دوره‌های گذرانده شده توسط اینجاب در حوزه شبکه، امنیت، سیستم‌های کنترل صنعتی و امنیت سیستم‌های کنترل صنعتی، عناوین و مدت و نام مدرس و همچنین موسسه آن‌ها را به تشریح در جدول زیر ذکر نموده‌ام.

جدول ۱. شناسنامه آموزشی اسماعیل باقری اصل

نام دوره/سمینار	مدت دوره (ساعت)	نام مدرس	نام موسسه
PWK	۳۰	استاد مستعدی	موسسه کهکشان نور
CEH	۴۰	استاد حق محمدی	موسسه ویستا

CISSP	۳۰	نیکخواه	موسسه سایبرتک وIsc۲
LPIC1	۵۰	حاج غلامعلی	خصوصی مرکز امنیت فناوری اطلاعات حفیظ
LPIC2	۶۰	مهندس خویشتندار	موسسه سایبرتک
GICSP SANS ICS410	۳۰	جاستین سل	SANS
CCNA	۴۸	مهندس شاملو	موسسه سایبرتک
CCNA Security	۱۲۰	مهندس خویشتندار	موسسه سایبرتک
CCNP Route & Switch	۱۱۰	شاملو	موسسه سایبرتک
HCNA	۴۰	خودآموز	خودآموز
JNCIA-Junos	۱۸	مهندس نظریان	موسسه ویستا
JNCIP-SEC	۳۰	مهندس نظریان	موسسه ویستا
JNCIS-SEC	۴۰	مهندس نظریان	موسسه ویستا
YOKOGAWA CENTUM CS 3000 R3/ Fundamental	۳۰	مهندس وطنخواه	مرکز امنیت فناوری اطلاعات حفیظ
YOKOGAWA CENTUM CS 3000 R3 Engineering	۳۰	مهندس وطنخواه	مرکز امنیت فناوری اطلاعات حفیظ
YOKOGAWA CENTUM CS 3000 R3 Maintenance	۲۰	مهندس وطنخواه	مرکز امنیت فناوری اطلاعات حفیظ
PLC - Siemens S7-300 Maintenance and Trouble Shooting	۴۰	مهندس هژبریان	قشم ولتاژ- خصوصی حفیظ
PLC - Siemens S7-400 Maintenance and Trouble Shooting	۵	مهندس هژبریان	قشم ولتاژ- خصوصی حفیظ
Siemens SCADA - WinCC	۳۰	مهندس هژبریان	قشم ولتاژ- خصوصی حفیظ
PLC - Siemens S7-300-400 TIA Portal | Programming	۳۰	مهندس هژبریان	قشم ولتاژ- خصوصی حفیظ
امنیت پروتکل‌های ارتباطی در سیستم‌های کنترل صنعتی	۵	پیمان گلشنی دانشجوی	انجمن رمز ایران

		دکترای دانشگاه صنعتی اصفهان	
سمینار شهر امن	۸	Dahua	شرکت فرا گستر
OPSEC for Control Systems	۱۰	E-learning	Department of Homeland Security's (DHS ICS-CERT)
210W-02 Cybersecurity for Industrial Control Systems - Influence of Common IT Components on ICS	۳۰	E-learning	Department of Homeland Security's (DHS ICS-CERT)
210W-03 Cybersecurity for Industrial Control Systems - Common ICS Components	۱۵	E-learning	Department of Homeland Security's (DHS ICS-CERT)
210W-04 Cybersecurity for Industrial Control Systems - Cybersecurity within IT & ICS Domains	۱۵	E-learning	Department of Homeland Security's (DHS ICS-CERT)

۱-۴- پروژه‌های انجام شده

- تدوین روشگان بومی تست نفوذ پذیری زیرساخت‌های کنترل صنعتی
- تدوین توصیه‌نامه بومی امنیت سایبری در زیرساخت‌های صنعتی
- تست نفوذ پذیری شبکه زیرساخت‌های حساس و حیاتی کشور که به علت حفظ محرمانگی از عنوان نام آنها پرهیز می‌شود.
- تحقیق و پژوهش در زمینه بدافزارهای سیستم‌های کنترل صنعتی از قبیل استاکس‌نت، شعله، دوکو و ...
- ارائه روش‌های شنود داده‌ها در زیرساخت‌های کنترل صنعتی
- ارزیابی امنیت و عملکرد دیوارآتش صنعتی شرکت امن پژوه نوآوران فارس
- ارزیابی امنیت و عملکرد نرم‌افزار اسکادای شرکت کرمان تابلو به همراه تمامی ماژول‌های آن
- تحقیق و پژوهش در زمینه بازبینی عمیق بسته‌ها در پروتکل‌های صنعتی(DPI)
- آموزش دوره امنیت سایبری در زیرساخت‌های کنترل صنعتی
- تحقیق و پژوهش در زمینه امنیت زیرساخت‌های صنعتی و سایبری
- ممیزی و ارزیابی امنیت زیرساخت‌های کنترل صنعتی و اسکادا با حضور در محل که از ذکر عناوین به علت حفظ محرمانگی پرهیز می‌شود
- تدوین روشگان تست‌نفوذ بومی در زیرساخت‌های فناوری اطلاعات و ارتباطات
- تست‌نفوذ پذیری زیر ساخت‌های حساس و حیاتی مرتبط به حوزه‌های فناوری اطلاعات و ارتباطات
- آموزش و مستندسازی ابزارهای تست امنیت سایبری در زیرساخت‌های سایبری و کنترل صنعتی
- طراحی آزمایشگاه امنیت شبکه

- ارزیابی و تحلیل آسیب‌پذیری‌های شبکه‌های سرگرمی و اجتماعی برون‌مرزی که به علت محرمانگی از عنوان نام آنها پرهیز می‌شود.
- طراحی و تولید مفهومی سنسور تشخیص نفوذ شبکه‌های صنعتی
- طراحی معماری مرکز عملیات امنیت زیرساخت‌های صنعتی/سایبری
- طراحی و تدوین راهکار جامع امنیت در زیرساخت‌های صنعتی
- طراح مرکز پاسخ‌گویی به رخدادهای صنعتی/ سایبری
- طراح و تولید سامانه ارزیابی سیاست‌های امنیتی در زیرساخت‌های صنعتی
- .....

۱-۵- مقاله‌های نگارش شده

[۱] خالقی(ح)،باقری اصل(الف)،جلالیان(ع)،صیاد(م)،(۱۳۹۳)،امنیت سایبری در سیستم های اسکادای زیر ساخت نفت و گاز (ریسکها و حملات سایبری). اولین همایش ملی ذخیره سازی زیرزمینی نفت و گاز

[۲] باقری اصل،(الف). (۱۳۹۵) بررسی آسیب‌پذیری‌ها در زیرساخت‌های حساس و حیاتی. مجله سما (پژوهشکده پارسا شریف)، پاییز ۹۵

[۳] باقری اصل،(الف). (۱۳۹۵) جرم‌شناسی در زیرساخت‌های کنترل صنعتی. مجله سما، زمستان ۹۵

[۴] باقری اصل،(الف). (۱۳۹۶) مرکز عملیات امنیت صنعتی(چالش‌ها و ضرورت‌ها). مجله سما، بهار ۹۶

[۵] باقری اصل،(الف). (۱۳۹۶) تفاوت رویکرد امنیت در زیرساخت‌های فناوری اطلاعات و کنترل صنعتی. مجله سما، بهار ۹۶

[۶] باقری اصل،(الف). (۱۳۹۶) بازرسی امنیت پیرامونی، ارزیابی سیاست‌ها یا تست نفوذ در زیرساخت‌های صنعتی کدام بهتر است؟. مجله سما، تابستان۹۶

[۷] باقری اصل،(الف). (۱۳۹۶) معرفی طرح تولید محصول‌های مرتبط با امنیت زیرساخت‌های صنعتی. مجله سما (پژوهشکده پارسا شریف)، پاییز ۹۶

[۸] باقری اصل،(الف). (۱۳۹۶) مفهوم دفاع در عمق در زیرساخت‌های صنعتی. مجله سما (پژوهشکده پارسا شریف)، زمستان ۹۶

[۹] باقری اصل،(الف). (۱۳۹۶) زیرساخت‌های صنعتی کشور در انحصار برندهای غیر بومی. مجله سما (پژوهشکده پارسا شریف)، زمستان ۹۶

[۱۰] باقری اصل،(الف). (۱۳۹۶) حملات پایدار و پیشرفته در زیرساخت‌های حساس و حیاتی. مجله سما (پژوهشکده پارسا شریف)، زمستان ۹۶

[۱۱] باقری اصل،(الف). (۱۳۹۶) شناسایی، ارزیابی، تشخیص و پاسخگویی در زیرساخت‌های صنعتی(راهکار یکپارچه). مجله سما (پژوهشکده پارسا شریف)، زمستان ۹۶