Art Le Bel

Cyber Security Engineer & Architect · CISSP

art@artlebel.com · +1 (281) 505-0561 · Houston, TX · artofscripting.com · artlebel.com · github.com/artofscripting

Summary

20+ years across software development, end-user analysis, mass-data visualization and networking — with a career-long focus on automation, testing, and research-driven defense.

Experience

Cyber Security Delivery Manager
Jun 2024 – Present

Accenture Federal Services

- Conduct **security reviews of architecture diagrams** with project teams, identifying risks and recommending remediations aligned to security frameworks and best practices.
- Ran a **company-wide risk assessment** and now drive new technical projects representing the CISO office.
- Contributed to **NIST SP 800-218 (SSDF)** work and delivered technical solutions for **NIST SP 800-171** reviews — security-first, with minimal compliance overhead.

Director, Cyber Security Special Operations / Security Architect
Mar 2022 – Jun 2024

AMSYS

Lead security SME in an MSSP/MSP, consulting to **oil & gas, healthcare-data and banking** clients plus many SMBs. Built and deployed security programs with a hands-on, risk-based approach.

- Deployed WAFs for large auction sites, reducing **outages from daily to zero**.
- Designed and coded a custom **24/7 external attack-surface monitoring** solution.
- Reviewed **Darktrace** configuration and recommended custom ML modeling; monitored **CrowdStrike** detections via a custom intelligent-filtering dashboard.

Director of Information Security / Security Architect
Feb 2020 – Mar 2022

AMSYS

- Implemented and managed **security orchestration via APIs into Elasticsearch**; designed reporting dashboards for threat hunting, investigations, and status reporting.
- **Lead penetration tester** with Metasploit, OWASP ZAP, Burp, Nmap, Kali Linux, and custom Python web-app proxies across **GCP, Azure, and AWS**.

Lead Penetration Tester / Security Architect
May 2019 – Dec 2019

Royal Dutch Shell

- Processed **IRM assessments** targeting agile-developed applications.
- **Lead penetration tester** (Metasploit, ZAP, Burp, Nmap, Kali) with custom Python web-app proxies.

Security Engineer
Oct 2018 – Feb 2019

Disney

- Processed Data Protection Program (DPP) assessments targeting **EU and GDPR compliance**.

Security Architect, Software Author, R&D Lead
Feb 2017 – Jul 2018

SecurityKeys — RedLambda

SME for a **machine-learning-backed malware-detection product** built — initially — from Windows logs alone.

- Created a **log-centric streaming assessment process** for applications and end users; authored "behaviors" and signatures giving context to ML/AI algorithms.
- **Dissected malware into log-observable behaviors**; demonstrated privilege escalation, reverse TCP/shell, and RCE techniques to refine sensors.

Information Security Consultant
2016 – 2017

SecurityKeys

- Audited **hundreds of cloud applications for DoD use**; automated scanning with ACAS, Nessus, Nexpose, and WebInspect.
- Delivered **threat models and risk assessments** across PCI-DSS L3–4, NIST SP 800-37 RMF, FISMA, HIPAA, SANS CSC, SOX IT controls, and ISO.

Senior Information Security Engineer
Mar 2012 – Jul 2016

Ellucian (Datatel / SungardHE)

Partnered directly with Rapid7 to build one of the first large-scale multi-tenant, cloud-based vulnerability-management systems — **25,000+ critical devices across 60+ organizations**. Deployed VM for 50+ schools and **automated a full FTE's workload within six months**.

- Wrote custom Ruby scripts and proprietary gems to automate testing and reporting; built **custom payloads for near-zero-day vulnerabilities** such as Heartbleed.
- Worked with the AWS security team on a securable cloud migration; trained staff on Rapid7 (Nexpose, Metasploit) and core tooling. Became the **go-to cloud expert for 700 schools**.

Senior Information Assurance Engineer Brandon Technology Consulting — MHS/TMA (TRICARE) Sep 2011 – Jan 2012

Senior Information Assurance Engineer Lockheed Martin IS&GS — U.S. Air Force Apr 2010 – Sep 2011

Info. Management & Assurance Security Officer (IMO / IASO) U.S. Army — 3-159 ARB, 12th CAB, TF 34
Deployed · 2008 – 2009

Info. Management & Assurance Security Officer (IMO / IASO) U.S. Army — 12th CAB, V Corps, Illesheim, Germany
2007 – 2008

Certifications

CISSP (ISC)² · since 2012

CompTIA Security+ 2010

EMSEC / TEMPEST
U.S. Air Force certified

U.S. Army Signal Corps 2006

Education

A.S., Digital Media
Full Sail University — Orlando, FL
2001 – 2003

Advanced Space Academy
NASA — Huntsville, AL · "Right Stuff" Medal
2000

Awards & Decorations

Army Commendation Medal · Army Achievement Medal · National Defense Service Medal · Global War on Terrorism Medal · Iraq Campaign Medal, w/ Campaign Star · Army Good Conduct Medal · Overseas Ribbons · NASA "Right Stuff" Medal

Skills

Operating Systems: Windows, Debian, Red Hat, Fedora, Ubuntu, SUSE, Solaris

Platforms: MS Exchange, Oracle, SQL Server, IIS, Active Directory, VMware, Apache

Networking: Cisco, TCP/IP, DHCP, DNS, (S)FTP(S), SSH / Telnet, 802.11 a/b/g/n, AirFortress, QoS, Load Balancing, SMTPS

Security Tooling: Metasploit, Nessus, Nexpose, OpenVAS / Greenbone, Retina, Burp, OWASP ZAP, Nmap, Wireshark, Netcat, ngrep, Kismet, GFI LanGuard, AppDetective, WebInspect, ACAS

Cloud: AWS (CLI / SDK), Docker, Azure, GCP

Big Data & ML: Elasticsearch, MongoDB, Kafka, Kibana, Logstash, Spark, Neo4j, kNN, RNN, CNN, NLP

Scripting & Languages: Python, Java, PHP, Perl, Ruby, Bash, PowerShell, WSH, VB, JavaScript, C (IoT)

Threat Modeling: STRIDE, PASTA, TRIKE, Attack Tree, DREAD, Kill Chain, CAPEC

Frameworks & Standards: NIST SP 800-218, 800-171, 800-37 RMF, DIACAP, FISMA, HIPAA, PCI-DSS, SOX, ISO, SANS CSC, GDPR

Projects

LogRegulator, UltimateIP, Threat Signal Forge, Nginx Signal Forge, SOCtoys, AI Auditor Assistant, Pentesting-Team, HydraSocket, NewsReader & Research Workspace, Blockforge, UltimateIP Control