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.

I have worked at the Pentagon as a cyber security expert and supported large U.S. organizations from major educational institutions to the Department of Defense (DoD) and Office of the Secretary of Defense (OSD) — developing, maintaining, and reinforcing IT security systems to the highest standards. My approach pairs a software-development background with TTP research and behavioral-model development.

To sharpen detection, I apply software-engineering techniques to "big data" analytics using cost-effective data interrogation — writing high-speed algorithms (kNN, RNN, CNN, NLP) in Java and Python to surface layered, explanatory new data points, while keeping solutions efficient and cost-aware.

Experience

Cyber Security Delivery Manager
Accenture Federal Services

Jun 2024 – Present

Security Engineering, Architecture & Risk — CISO office

Senior technical resource to the CISO office on the Security Engineering, Architecture & Risk team.

- 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.
- Technical resource to the **Policy & Standards team**; performed policy assessments producing detailed technical-implementation and optimization recommendations.
- 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
AMSYS

Mar 2022 – Jun 2024

MSSP / MSP — Special Operations Consulting

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.
- Built **API push/pull integrations** to stream custom data such as firewall notifications into the SIEM.
- Reviewed **Darktrace** configuration and recommended custom ML modeling; monitored **CrowdStrike** detections via a custom intelligent-filtering dashboard.
- Served as **Tier 3 operator** for C-level cybersecurity concerns.

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

Security Program Manager for AMSYS and its clients.

- Implemented and managed **security orchestration via APIs into Elasticsearch**; designed reporting dashboards for threat hunting, investigations, and status reporting.
- Reviewed system diagrams, interviewed stakeholders, and documented findings, remediation plans, and **DevSecOps process optimizations**.
- **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
Royal Dutch Shell
May 2019 – Dec 2019
Short-term contract

- Processed **IRM assessments** targeting agile-developed applications.
- Reviewed diagrams, interviewed stakeholders, and documented findings, remediation plans, and **DevSecOps optimizations**.
- **Lead penetration tester** (Metasploit, ZAP, Burp, Nmap, Kali) with custom Python web-app proxies.

Security Engineer
Disney
Oct 2018 – Feb 2019
Security Compliance Consulting — short-term contract

- Processed Data Protection Program (DPP) assessments targeting **EU and GDPR compliance**.
- Reviewed diagrams, interviewed stakeholders, and documented findings, remediation plans, and process optimizations for DPP.

Security Architect, Software Author, R&D Lead
SecurityKeys — RedLambda
Feb 2017 – Jul 2018
Software Development Consulting

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.
- Built **cloud, hybrid, and on-prem deployments** (AWS, Docker, AWS CLI/SDK).
- Coded in **Python, Java, PHP, JavaScript, Bash, and PowerShell** with Elasticsearch, MongoDB, Kafka, Kibana, Logstash, Spark, and Neo4j; Agile via Jira/Confluence.

Information Security Consultant
SecurityKeys
2016 – 2017
Information Assurance — TRICARE Management Activity, Navy MWR

Traveled the U.S. conducting **Security Technical Implementation Guide (STIG) audits** and application security reviews across mixed-technology network implementations.

- **Senior on-site consultant** responsible for final data collection, review, and report delivery.
- Audited **hundreds of cloud applications for DoD use**; automated scanning with ACAS, Nessus, Nexpose, and WebInspect.
- Conducted **static code reviews** for Agile/Scrum environments (Java, PHP, .NET, proprietary).
- 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
Ellucian (Datatel / SungardHE)
Mar 2012 – Jul 2016
Lead Vulnerability Engineer

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**.

- Conducted DoS (virtualized DDoS), **local privilege escalation, RCE, and web-app reviews** (database, static/dynamic source, fuzz/SQLi).
- 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

- Prepared C&A reports for senior officials using the **DoD DIACAP process** for commercial and government networks.
- SME on .NET, IIS, Apache, UNIX/*nix, SharePoint, and databases (MS/MySQL, DB2, Oracle).
- Trained personnel on HP Security Suite, Retina, AppDetective, Burp Suite, and WebInspect.

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

- Prepared **C&A reports for senior Air Force officials** via DIACAP and the IT-Lean process.
- **Lead Retina Remote Enterprise Manager administrator**; tuned enterprise network scanning performance.
- Certified in Emission Security; managed **TEMPEST security for National Capital Region units**.
- Wrote **application risk assessments** using IBM Rational AppScan and proprietary USAF scripts; built tooling for managerial visibility and standards.

Info. Management & Assurance Security Officer (IMO / IASO)
U.S. Army — 3-159 ARB, 12th CAB, TF 34
Deployed · 2008 – 2009
Service Oct 2006 – Mar 2010

Maintained **300+ combat-operations computers** across multiple networks supporting AH-64 (Apache) operations; became the deployed cyber-warfare SME.

- Engineered a **1.5-mile Wi-Fi link** relaying real-time test-pilot data to the Battle Captain and commanders; maintained the **largest map server deployed (2009)**.
- Created **custom software** to investigate and document vulnerability and security events; identified major threats before zero-day.
- Delivered **100% uptime** to critical users across multi-segment networks.

> Medically retired for combat-zone injuries — with awards, medals, and honors.

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

IT SME managing digital training environments for 3-159 ARB operations — remote data management, real-time networking, and security systems — for **400+ users**.

- Built the **most realistic network-training environment** for commanders, pilots, and users with upper leadership.
- Maintained McAfee Enterprise, Active Directory, software inventories, and Cisco networking; trained IT/radio staff in AD management and security risk.

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

Cisco & Linux coursework
Routing, switching, VoIP, PIX security, SNMP; Linux CLI, regex & text processing

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
logregulator.com

UltimateIP
ultimateip.info

Threat Signal Forge
threatsignalforge.com

Nginx Signal Forge
threat.ultimateip.info

SOCtoys
soctoys.com

AI Auditor Assistant
aiauditorassistant.com

Pentesting-Team
pentesting-team.com

HydraSocket
hydrasocket.com

NewsReader & Research Workspace
news.artlebel.com

Blockforge
codeblockforge.com

UltimateIP Control
users.ultimateip.info