

Christopher La Fleur

Uxbridge, Hillingdon, UB8 2UW
www.linkedin.com/in/chris-la-fleur-a7371a133
Mobile Number - 07463170485
Email: Christopher.lafleur@owasp.org
[Website](#)
[YouTube Channel](#)

Artificial Intelligence and Cyber Security Architect

An innovative and trustworthy subject matter expert proficient in all fields!

Committed to identifying and defining requirements that support organizational goals through strong leadership and effective collaboration. Demonstrated success in critical thinking, problem-solving, and decision-making, supported by excellent communication skills.

- *AI and Cyber Security GRC over Hybrid Architecture* • *Embedded Data Security GRC*
 - Global Security Standards Implementation for Regulatory and Legal Compliance
-

TECHNICAL PROFICIENCIES

Environments	Private, Public, Hybrid and Community Cloud (AWS, Microsoft Azure, Google) and OT spaces, On premise and endpoint SASE security includes Windows, Unix and Citrix OS's, Cisco Networks, M365 Suite, Lucent, QIP DNS and DHCP (also including WINS) deployment, management and support.
Cybersecurity Tools, Technologies, Deployed	GISKARD A.I vulnerability scanner (New), Microsoft Purview, CyberArk, Windows Defender Security Center & Sentinel, Splunk & Alien Vault SIEM, Trend Micro Enterprise Suite, WireShark, Tenable Vulnerability Scanner, FortiGate 500c Firewall, Cisco ASA, Netscaler /Zscaler Citrix Gateway, RSA Authentication Manager, Sonicwall, Checkpoint Firewall version - r80, PALO ALTO, Big IP, McAfee, and Blue Coat Web Proxy Server, Active Directory, Cisco Pix Firewall, CSACs, Netscreen Firewall, Cisco SNS NAC Tool, Cisco Nexus Routers/Switches for LAN and WAN topologies, Netscout Packet Sniffer, Service Now Ticketing System VitalSuite, Netflow Tracker, Sonicwall, MIMESweeper, Websense URL Filter

...Continued...

PROFESSIONAL EXPERIENCE

Cybersecurity, Cloud, IoT & AI Security Architect — (Seconded from National Grid to National Gas)

National Gas is a UK Operator of Essential Services (OES) and part of the nation's Critical National Infrastructure (CNI), providing critical gas transmission services and operating within a high-threat environment.

Key responsibilities include:

- Design, deploy, and provide lifecycle support for cybersecurity and artificial intelligence security solutions across a critical national infrastructure environment.
- Serve as a technical authority on the Technical Design Authority (TDA) panel, conducting peer reviews and assuring the security, resilience, and compliance of major projects.
- Apply emerging AI governance and security practices using frameworks and standards including **NIST AI RMF 1.0 (NIST AI 100-1)**, **NIST AI 600-1**, and **ISO/IEC 42001:2023**.
- Conduct internal audits, inspections, and assurance reviews to verify that projects comply with organizational security procedures and applicable AI governance requirements.
- Develop cloud security and IoT architectures aligned with **ISO/IEC 27001**, **ISO/IEC 27017**, the **NCSC Cyber Assessment Framework (CAF)**, and the **NCSC 14 Cloud Security Principles**.
- Successfully delivered and supported more than **50 complex security and technology projects**, including the design and successful implementation of National Gas's first IoT solution.
- Perform **STRIDE threat modelling** and apply **MITRE ATT&CK** methodologies to strengthen security controls, identify attack paths, and improve defensive measures.
- Manage environmental, AI, and application-security vulnerabilities using **SAST** and **DAST** practices, producing risk assessments, remediation plans, and lessons-learned documentation through to formal closure.
- Communicate effectively with internal and external stakeholders, translating complex technical and security risks into clear, actionable recommendations.
- Recognized as a highly collaborative, technically capable, supportive, and solutions-focused professional.

- Serve as a member of the Technical Design Authority (TDA), evaluating and approving the addition, removal, and modification of security controls to support optimal technical and business outcomes.
- Provide cost-effective, risk-aligned security solutions to solution architects for both high-level and low-level designs.
- Review SaaS, PaaS, and IaaS solutions from both user and service-provider perspectives, applying control frameworks aligned with **NERC-CIP, NCSC CAF, CSTAR, NIST SP 800-53, ISO/IEC 42001, and ISO/IEC 27001.**
- Act as the Senior Security Architect for change-control activities, ensuring that proposed changes meet security, risk, and compliance requirements.
- Liaise between Legal and Risk teams to support the assessment, management, and resolution of security and compliance matters.
- Coordinate and scope initial and annual penetration-testing exercises, reviewing findings and prioritising remediation activities.
- Define vulnerability-management schedules and coordinate the prioritised remediation of identified security weaknesses.
- Translate and negotiate security-framework requirements between management and technical stakeholders, including Windows, Unix, database, third-party supplier, and solution-architecture teams.
- Oversee the deployment and integration of security capabilities, including antivirus, access control, content inspection, file-integrity monitoring, privileged-access management, machine learning, firewalls, API security, multifactor authentication, and Prisma Access/SASE endpoint security.
- Implement **MITRE ATT&CK**-aligned logging and monitoring using Microsoft Sentinel and Splunk, including the use of brokers and subscription-based integrations across the enterprise.
- Support incident-management activities, including the coordination, investigation, escalation, and resolution of security incidents.

Cyber Security Engineer for Atradius (March 2022 – Dec 2022)

Atradius is a European, multi-billion-euro provider of global credit-management services operating within a highly regulated financial-services environment. As a member of a four-person security team, I was responsible for implementing and maintaining Governance, Risk, and Compliance (GRC) practices across the organisation.

Key responsibilities were:

Christopher La Fleur

Page Two

- Ensuring alignment with applicable regulatory and industry requirements, including the **Sarbanes–Oxley Act (SOX), GDPR, DORA, and ISO/IEC 27001**.
 - Assessing existing technical security controls and identifying requirements for new or enhanced capabilities.
 - Managing the procurement of security technologies, professional services, and vendor solutions.
 - Supporting incident response and coordinating security-related investigations and remediation activities.
 - Providing security-architecture guidance across business and technology initiatives.
 - Managing multiple security projects from initial planning through delivery.
 - Collaborating with internal stakeholders and third-party suppliers to improve security governance, risk management, and regulatory compliance.
- Designed and enhanced security controls aligned with ISO/IEC 27001 Annex A controls—including A.5, A.6, A.8.3, and A.9.2 onwards—and the NCSC Cyber Assessment Framework (CAF).
 -
- (Cont...)
- Strengthened the organisation's security posture by implementing vendor-recommended best practices and improving the effectiveness of existing defensive controls.
 - Designed, documented, and implemented enhanced logging and monitoring capabilities to support incident detection, investigation, and response.
 - Identified mitigations for known and underlying security issues and secured funding through the preparation and submission of Business Initiation Documents.
 - Introduced MITRE ATT&CK-aligned logging requirements for Windows domains, enabling the ingestion and analysis of relevant security events within the SIEM platform.
 - Conducted current-state assessments, threat modelling, and forward-looking security analysis to inform cybersecurity improvements and investment priorities.
 - Led the planning and security design of Zero Trust and Secure Access Service Edge (SASE) capabilities across nine globally distributed remote offices.
 - Implemented data discovery and classification activities to support data-privacy requirements and reduce the risk of data leakage.

Cyber Security Specialist – for the UK Police, Public Protection Home Office Unit

I led the NIST PRISMA information-security programme review for the Police National Computer Security Operations Department, improving the maturity of operational practices designed to safeguard highly sensitive data processed and stored across several UK criminal databases to strengthen preparedness for cyberattacks. I enhanced governance, threat modelling, vulnerability management, and the security of legacy and cloud infrastructure. I also introduced MITRE ATT&CK-aligned SIEM capabilities and improved knowledge transfer through structured documentation and workflows using Confluence and Jira.

Key Achievements:

- Audited and assessed Security Operations against NIST PRISMA directives, conducting a comprehensive gap analysis and documenting recommendations, improvements, and lessons learned.
- Integrated security activities into Agile delivery methodologies, supporting high-quality service delivery across Police and Public Protection projects throughout the secure development lifecycle.
- Provided expert guidance on supply-chain security and implemented Web Application Firewall (WAF) solutions alongside SIEM architecture incorporating host- and network-based logs for enhanced threat detection and analysis.
- Led organisation-wide investigations into Log4j vulnerabilities, assessing risks across affected functions and components and coordinating remediation activities.
- Improved security awareness among security teams and directors through Confluence-based knowledge sharing and regular open security forums.
- Implemented MITRE ATT&CK-aligned logging standards across Windows domains and enhanced protective monitoring for cloud orchestration environments.
- Collaborated with stakeholders to assess the overall security programme using PRISMA, helping measure maturity, strengthen security practices, and drive continuous improvement.

OFGEM - Cyber Security Specialist (2018 - 2021)

I Performed security gap analysis to determine inadequate or limited security controls and configurations. I was the first in a considerable amount of time to uncover underlying vulnerabilities previously not detected before, which drove a complete redesign and implementation of Microsoft Ever Green's architecture. Completed Nessus vulnerability assessment and threat modeling on internal and external assets to drive quality and efficiency. Led DLP configuration and administration, enforcement of machine learning controls, disk encryption on mobile devices, and remote wipe controls.

Note: Please also see my [YouTube](#) video of an event which took place whilst working at OFGEM

Christopher La Fleur

Page Two

Key Achievements:

- Championed Agile methodologies to enhance service delivery and support the successful execution of security initiatives.
- Recognised as a subject-matter expert in security operations spanning the secure development lifecycle (SDLC), network communications, vendor management, procurement, and Cyber Incident Response Team (CIRT) activities.
- Led the enterprise-wide migration of two Advanced Persistent Threat (APT) monitoring and prevention appliances, strengthening the detection, prevention, and reporting of suspicious activity.
- Introduced improved security incident-response processes using Syslog data, event-reporting groups, and a purpose-built security incident-response playbook.
- Hardened internal and cloud-hosted operating systems by assessing CVEs and severity scores from the National Vulnerability Database (NVD), with comparative analysis against OWASP Common Vulnerability Scoring System (CVSS) assessments.
- Served as a methodical Security Advisor for Microsoft Azure migration projects, ensuring GDPR requirements and NCSC guidance were applied to the handling of sensitive data

Bank Security Architect AVP (2017 - 2018)

Barclays Bank

Single handedly I designed and implemented of the Barclays online Whistle-Blowing datacenter for public facing online interaction with internal and external entities and members of the public using Zero Trust safeguards. I concurrently proactively diagnosed and resolved complex network and security issues through Wireshark and packet-capture analysis, while detecting and mitigating threats such as DoS, DDoS, SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) using intrusion prevention systems (IPS). Documented recovery time objectives (RTOs) and recovery point objectives (RPOs) for disaster-recovery testing and presented findings to external stakeholders to support informed decision-making and problem resolution. Led the migration and configuration of PRTG Network Monitor across network devices using SNMP and standard TCP ports, while administering Windows Active Directory and WSUS across diverse environments, including Windows Server OS's, DNS, Cisco Catalyst switches, and high spec Firewalls. Architected and engineered FortiGate firewall deployments, designing and implementing granular security policies using RADIUS, TCP/IP, UDP, secure VLAN segmentation, HTTP, HTTP, HTTPS, DNS, SSH, custom ports, and dynamic and static NAT assignments.

Key Achievements:

- Architected and deployed RSA Authentication Manager across the global WAN, managing software and hardware tokens for more than 50 users and securing access to confidential data.
- Strengthened network security through segmentation using NetScaler, Cisco router and switch security best practices, and strategically deployed Firewall technologies.
- Integrated comprehensive firewall logging and monitoring with the Security Operations Centre (SOC), improving security visibility and operational response.
- Enhanced security detection, prevention, reporting, and traffic-segregation controls based on defined access criteria.

- Appointed Project Manager and Security Architect for the modernisation of the legacy network infrastructure.
- Produced clear, user-focused technical documentation and operational manuals, enabling support teams to manage and maintain implemented technologies effectively.

Senior Network Security Engineer and Analyst (2010 - 2017)

Deutsche Bank

Responsible for the support and administration of Check Point, Palo Alto and Juniper firewalls with an IDS managed through a Defense Center, McAfee Web Gateway, Cisco routers and switches, and Blue Coat proxy servers. Created and deployed firewall security policies and protocols, including VPN implementations and high-availability configurations. Utilised NetScout packet-capture devices, Wireshark, NetGrapher, NetFlow, CW2K, and ServiceNow to build operational capacity, coordinate change, and minimise risk across vulnerable environments and transitional stages. Provided hardware and software support and maintenance for Cisco Nexus 3K, 5K, and 7K series platforms across data-centre environments. Ensured optimal connectivity and network performance across multiple circuits, TCP/IP routing, multicast, and QoS communications.

Key Achievements:

- Assumed an influential role in bringing forth significant architectural changes from close monitoring and enhanced vigilance.
- Appointed as a Global Team Leader for ASIA/PAC Europe because of demonstrating subject matter level expertise in network and application security.

1st Line Support Engineer (2006 - 2010)

Deutsche Bank

Provided multi-level support in monitoring and re-mediating issues across the network infrastructure. Served as a primary contact in interfacing with escalated clients to resolve problems and liaised between banks and ISPs to report circuit failures and restore service. Honed expertise in Wintel, Unix, Storage, Firewall, routing protocols with load balancing and HSRP mechanisms to establish a reputation as a tactical fault finder and master incident manager.

Key Achievements:

- Led the configuration of internal and external hosts to bolster communication methods across dynamic environments.
- Composed training guides and learning materials to assist teams in executing investigations.

Senior Network Analyst (2002 - 2006)

Cheshire Data Systems

Assembled and activated Apache and Windows IIS Servers, utilizing Compaq servers to reinforce robust hardware builds. Generated PKI infrastructures along with domain name assignment & renewal, public certificate granting, and online transaction security measures. Augmented Cisco Router ACLs and security policies on Checkpoint Firewall, Watchguard, and Netscreen Firewalls, NAT, PAT, Anti-Spoofing, and VPN circuits security policy design and implementation. Executed DNS changes on global A records and domain names, proliferating

Christopher La Fleur

Page Two

an in-depth knowledge of DNS PTR records where required. Conducted incremental and differential backups of web servers for secure storage using ArcSight suite.

*Additional professional experience includes **Network Security Consultant, Network Analyst, Forensics Engineer, and Field Engineer.***

EDUCATION AND CREDENTIALS

ISO/IEC42001 Lead Implementer

ISO/IEC27001 Lead Implementer

CISSP

CISM

CEH v9

Palo Alto PCNSE

CCSA

CCNP

MCSE

PRINCE2