**Krishan James Shaw**  
**66 Raynel Drive, Leeds, LS16 6BP**  
**07563 498 068**  
**email – krishshaw@live.co.uk**

**TECHNICAL EXPERIENCE**

* Active Directory Administration (User account creation, Security & Distribution group creation, OU creation & management)
* Microsoft Exchange Management – Mailbox creation and management
* Windows XP, 7, 8.1 & 10 Desktop Support
* Microsoft Server, 2008 R2 & 2012 R2 patching via WSUS
* Ubuntu Linux 14.04 – 18.04 management
* File share & permission management on Microsoft Servers
* SCCM (Deployment of software packages)
* Citrix Desktop administration
* Antivirus deployment and administration (Sophos, Trend, Mcafee)
* RSA Secure ID administration
* Mimecast administration
* Desktop & Laptop builds
* Use of monitoring tools (Nagios, Solarwinds, Netflow, PRTG)
* Use of Service Management Tools (Remedy, HP Service Manager, ManageEngine, ServiceNow)
* LogRhythm SIEM (AIE Rule creation & management, alarm investigation, reporting)
* LogRhythm SIEM (Server patching, failover using SIOS Lifekeeper)
* ELK stack maintenance and management
* Nexpose / InsightVM Vulnerability Scanners
* Censornet Web Proxy & CASB
* Understanding of networking technologies

# EMPLOYMENT HISTORY

**Information Security Analyst**

Covea Insurance

August 2018 – September 2019

Covea Insurance operate in the UK offering commercial, motor, high net worth, property and protection insurance. Following a period of change, a new InfoSec team has been created which has a SecOps team.

Responsibilities:

* Vulnerability Management - ensuring all devices are being scanned and appropriate remediation plans are being put in place
* Management of the SIEM tool – ELK stack by Elastic.
* Management of Trend and Sophos antivirus solutions
* Responding to SIEM alerts and following the run book to investigate.
* Reviewing IPS alerts and tuning as required.
* Mimecast administration
* Using Netwrix and AD auditor to monitor user activity
* Assisting with DSAR and GDPR requests
* Weekly review of IPS rule hit using CheckpointManager R80
* Administration of the web proxy & CASB
* Monitoring of DLP alerts
* Currently leading the RFP process for to source a Managed SOC

**Security Analyst**

Capita Cyber Security

September 2017 – August 2018

Capita IT Enterprise (ITES) is a division of Capita and is presently Britain’s largest provider of IT solutions. Capita ITES manages major IT infrastructure projects across the UK both internally for Capita organizations and to external clients. This is a 1st line support role within the Cyber Security Division providing managed SIEM solutions and support.

Responsibilities:

* Ensure all tickets are logged correctly via email, telephone and self-service portal.
* Run scheduled reporting and backup tasks, weekly and monthly.
* Ensure change management processes are followed where required.
* Assist with the identification and management of problem tickets.
* Using the LogRhythm SIEM tool, perform administration and configuration of the customer solution.
* Providing a technical explanation of a SIEM event to a customer.
* Analysis and correlation of events to determine if a breach has occurred.
* Where required escalate SIEM alarms to customer technical teams.

**Service Desk Manager**

Savills Plc

November 2015 – July 2017

Savills plc is a global real estate services provider listed on the London Stock Exchange. They have an international network of more than 700 offices and associates throughout the Americas, the UK, continental Europe, Asia Pacific, Africa and the Middle East. This role encompasses the management of the EMEA IT Service Desk, Mobile Support and Application support teams.

Responsibilities:

* Ensure the resolution of all IT incidents and service requests within agreed Service Level Agreement
* Adherence and development of internal SLA’s
* Member of the Change and Problem Management boards.
* Liaise with stakeholders in the business, build positive working relationships with the operational leads and the office managers
* Develop and Implement ITIL processes and procedures around incident, request, problem and change.
* Major Incident Management, driving return to service through support tiers and managing communication to both internal and external stakeholders.
* Development of team members, including both technical and soft skills through mentoring and training.
* Continual Service Improvement to look for ways to improve the overall support services to Savills.
* Provide support for Savills core LOB applications/services.
* Responsible for IT knowledge management & CMDB to ensure the necessary information is up to date and is available to the right people at the right time

|  |
| --- |
| **Service Desk Manager / Service Manager**  IDE Group - May 2012 – November 2015  Daisy Group (formerly Phoenix) - July 2011 – May 2012  Ide Group are a London based provider of managed IT solutions, who specialize in service desk support. They were awarded the contract I previously worked on at Daisy Group and I was asked to come down and assist with the transition of the contract by the client, a role which led to me being appointed the Service Desk Manager and eventually the Service Manager on the account.  The role was previously outsourced to Daisy Group and I moved to IDE Group under tupe.  Responsibilities:   * Providing initial 121 and group training to the new service desk on client process & infrastructure. * Managing ad hoc project teams on and off site. * In addition to the standard service desk, day to day management of two on site engineers based at a client site. * Develop and implement a new service desk structure that would meet the client needs for both call answering and call resolution. * Working to the clients requirements, develop and implement a strategy to shape and move the desk forwards to meet demands for future projects and processes. * Provide 3rd line support to the team and assist with pro-active monitoring of the clients server estate. * Champion Service Standards policy amongst the business, aimed at continually improving customer service to both internal and external parties. * Attend the weekly problem forum and change approval board meetings. * Oversee and complete monthly desktop and server patching. * Produce daily, weekly and monthly MI for internal and client use. This information forms the basis of monthly service reviews which I lead. * Manage ticket volumes across all resolver groups, with specific focus on aged tickets / tickets close to SLA breach. * Working with the client and internal stakeholders to develop the contract with a view to move to a more SIAM based model.   **Manager**  Enact Conveyancing Ltd - 2001 - 2011  Enact are one of the leading conveyancing companies providing a wide range of legal & I.T services to high street banks, building societies, estate agents & consumers.  I spent 10 years working at the company, working my way up during this time from a case handler to manager of a remortgage team. |
|  |

**EDUCATION & TRAINING**

* Park Lane College – BTEC National Diploma in Computing - Merit
* Queen Elizabeth Grammar School – 9 GCSE’s A – C
* ITILv3 – Foundation

**Availability – Immediate**