Rhys Evans

Passionate DevSecOps Leader & Ethical Hacker
rhys@rhysevans.co.uk | 07805 595190

PERSONAL SUMMARY

A high calibre **security professional** with a proven track record of leading, architecting & implementing secure & self-healing solutions that scale using methodical, diligent and applied strategic thinking placing importance on **people & culture**, **process** then technology.
An enthusiastic **leader** able to build & empower teams that can deliver at pace incorporating & leveraging effective **DevSecOps** practices.
An individual **passionate about ethical hacking**, technology, **GitOps**, **DevSecOps**, source control, infrastructure/documentation **as code**, Continuous Integration/Delivery/Deployments & effectively breaking silo's through **collaboration**.
A high achieving, multi-disciplined individual spanning across web, virtualisation & containerisation stacks.
A **clear communicator**, comfortable decision maker and **leader** able to build, challenge and support teams & organisations through **digital transformations**.

Thrive & excel at tackling complex challenges taking ownership of projects, problems or tasks.

Has a broad exposure to many technologies across numerous industries including public sector, manufacturing, health, financial institutions and central UK Government.
A technology agnostic trend follower in the container ecosystem, AWS, Azure, Office365 and recently "serverless" technologies such as AWS Lambda, Azure Functions and Kubernetes native services.

Regular attendee at meetups immersing in the wider communities.

CAREER SUMMARY

Flexciton | London

DevSecOps Practice Lead *May '20 – Present*

Flexciton is a startup building a product to optimize semi-conductor wafer fab machine utilization through AI (ML) technology.
As a practice lead and DevSecOps engineer the responsibilities include;

- Point of contact for all security related matters
- Built a secure file sharing micro service leveraging Azure ServiceBus, Azure Storage (TTL-bound SAS URI's) Pod Managed Identities, Azure Postgres, Azure Firewalls
- Built private Azure Kubernetes clusters to remove cluster worker nodes and private link endpoints being exposed to public internet leveraging Azure firewall and multiple k8s ingress
- Built a single consolidated observability framework (ELK, Azure Monitoring, Thanos.io (Prometheus, Grafana, AlertManager) spanning multiple Azure Kubernetes clusters leveraging Azure services (Azure Event Hub) for guaranteed log delivery
- Implement a modern CI/CD strategy using declarative Kubernetes & GitOps pipelines through FluxCD & Helm
- Build out a 'blue team' strategy i.e. mitigate OWASP Top 10, ensure cloud and application SIEM logs exist and audible
- Perform security reviews highlighting and resolving areas of risk

Key Skills

CORE EXPERTISE

- Passionate about DevSecOps
- Community Builder
- Leadership & Direction
- Conference & Meetup Speaker
- DevOps Transformations
- Micro-services
- Cattle Infrastructure
- Scaling Cloud-native Architecture
- Self-healing Architecture
- 12Factor App Evangelist
- Red Teamer
- Shift-left Empowerment
- Kubernetes Security
- AWS
- Azure
- Terraform, Packer
- Dotnet Core
- Git / VSCode
- Kafka/Zookeeper
- ELK/Opendistro/Splunk
- CI/CD Stacks (Drone/Jenkins)
- GitOps
- Gitlab/BitBucket/Github
- Business Stakeholder Management
- Chaos Engineering
- Rapidly adapt to changes & demands

CONTAINER STACK

- Kubernetes
- AKS/EKS
- Kubespray
- Docker EE (Swarm + K8s)
- Helm
- Docker/podman
- CRI-o
- Skopeo

BUILD STACK

- Ansible
- Nexus/Artifactory
- Jenkins
- Drone CI
- Packer
- Docker/Buildah
- Skopeo
- Helm

PROCESS/DEPLOY STACK

- Ansible
- Helm
- GitOps – FluxCD
- Drone CI
- Consul, Consul Template
- Terraform
- Flagger - Canary, A/B Deployments
- Agile/SCRUM + Ceremonies
- Collaboration Tooling Integration

OBSERVABILITY STACK

- ELK/Opendistro
- Grafana/Thanos
- Prometheus/Alert Manager
- Sysdig
- Splunk
- Distributed Tracing - Istio*
- ChatOps

DEV STACK

- Dotnet Core
- Java*
- AWS SNS,Lambda,SQS
- Learning Go
- RabbitMQ
- Azure Event Hub
- Azure Service Bus
- Fission.io

CAREER SUMMARY (cont.)

- Nurtured a cloud-native and event driven micro-services mindset amongst the developers whilst catering for cloud cost efficiency
- Implement security governance & policy for all aspects of the business and product services
- Funnel years of application and architecture security experience to secure both the business and product
- Socialise good security practices through workshops at early stages of developments ("shift-left")
- Review product and mitigate security risks with 'best practices' in micro-service architecture e.g. JWT RS256 Authn/z and Istio to enforce
- Adapt logging to expose structured event-based logging for added value and ease of monitoring/alerting for developers

Capgemini | London

A global leader in consulting, technology services and digital transformation. A multicultural company of over 200,000 team members in more than 40 countries.

Principal Platform Architect — *Jan '20 – May '20*

Senior Platform Engineer — *Aug '18- Dec '19*

- Managed & led a number of project teams exceeding 10 members on central Government projects requiring 24x7 & 99.999% SLA
- Recruited for and grew high performing teams
- Managed stakeholders, deliverables introducing & socialising agile/sprint to traditional IT stakeholders to also improve culture
- Ensuring team members were empowered, accountable and engaged on a personal level with weekly 1-2-1, identifying & ensuring individual motivations are captured & challenged appropriately
- Advocate & champion of effective collaboration/DevSecOps
- Host workshops to fill technical skill gaps & drive technical creativity
- Successfully penetration tested a global AWS Lambda RDS-backed SPA – found multiple API vulnerabilities
- Drove public/private cloud cost saving initiatives leveraging existing technology stacks in the 7 figures of magnitude
- Encouraged and empower team members to contribute back to upstream projects and the wider open-source community
- Identify and deliver on business requirements
- Integrated F5 & MetalLB with K8s Ingress
- Introducing K8s HPA custom metrics from Sysdig to tune the cluster autoscaler
- Deployed scalable Zookeeper/Kafka clusters on K8s
- Resourcefully built upstream Kubernetes stacks in air-gapped environments
- Implement open source projects - Thanos, Longhorn, cert-manager, MetalLB & Istio
- Implemented GlusterFS/Heketi, Ceph, Longhorn PoC's to provide persisted state in on-premise K8s clusters
- Leveraged open source tooling to enhance secret sharing, e.g. GPG, blackbox, keybase
- Supported & evolved centralised ELK solutions to rapidly auto-scale & more efficiently cope with log shipping at scale
- Part of a small team that supported Kubernetes workloads of >30k containers

SECURITY SKILLSET

- CiSP Member
- PKI (Vault, openssl, Microsoft CA)
- Metasploit
- OWASP Top 10 practitioner
- GPG/Blackbox
- Aircrack suite
- ZAProxy
- Nessus
- XSS
- PowerSploit
- SSO - OAuth/OpenID Connect/JWT/SAML2
- Sqlmap,Ettercap,ssldump,sslstrip,sslsplit,arpspoof,sslscan, Nmap,netcat,dnsse c2,Armitage, SET, Bloodhound
- Kubesec.io
- Fiddler
- Aqua microscanner
- Anchor/Clair
- Hackthebox member
- Scap
- Wireshark/tcpdump
- K8s OPA

LINUX SKILLSET

- Kali Linux
- Ubuntu
- SELinux
- Alpine
- CentOS
- RHEL
- CoreOS

CLOUD STACKS

- AWS
  - RDS, Lambda, EKS, ECS, S3, VPC, DMS, Cloudfront, API Gateway, DynamoDB, EC2, SNS, SQS, CloudTrail, ECR
- Azure
  - ServiceBus, Storage, EventHub, EventGrid, AKS, Postgres Managed Identities, ACR, Private Links, Functions
- vDirector/vSphere

QUALIFICATIONS & TRAINING

Splunk University — 2017

- Fundamentals 1
- Fundamentals 2
- System Administration
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Architecting Splunk Enterprise

Pluralsight — 2017+

- Architecting Microsoft Azure Solutions
- Securing Cloud DevOps in Paas, Iaas SaaS
- Continuous Integration with Jenkins
- Continuous Delivery with Docker & Ansible
- Using Docker on AWS
- Implementing Windows Server SDN

Cyberoam — 2011

- CCNSP

Swansea University — 2006-2009

- BSc Hons Computer Science

CAREER SUMMARY (cont.)

Capgemini | London (cont.)

- Successfully pen-tested a client API exposing multiple vulnerabilities drove fixes to resolution while managing stakeholders
- Containerised traditional based services deploying to Kubernetes Introduced Open Source alternatives to commercial products
- Multiple effective & accurate RCA conclusions

Intelliflo | London

Intelliflo are a SaaS provider to over 2,000 financial advisory firms including Nationwide, Legal & General and Chase de Vere. Totalling c. 20,000 end customers and managing over £350 billion worth of financial assets. Key achievements & responsibilities include:

- Hosted workshops centralise technical knowledge and expertise (PowerShell (incl. DSC) + SQL Server)
- Continuously evangelised automation (DevOps) practices
- Achieved further business value from existing tool stacks Implemented corporate tooling on AWS ECS
- Implemented resilient HA services e.g. Always-on OpenVPN integration with two-tier PKI
- Centralised script & task orchestration
- Successfully automated the migration of the entire SaaS virtual estate from VMware to SCVMM
- Manage & support multi-site SCVMM private infrastructure
- Automated the implemented 'internet based' SCCM to streamline management of the Windows estate
- Integrated Intune with SCCM for iOS / Android MDM management & certificate distribution via NDES
- SCCM, Windows, Office365 & AD SME
- Improve & streamline the Agile / Scrum environment / workflows

SCC | Cardiff & relocation to London

SCCM & PowerShell SME *Apr '16 - Aug '16*

Providing automated solutions for London based NHS hospitals for a large EUC (Windows) project roll out of c. 20,000 devices.

Data Centre Automation Engineer *Feb '15 - Apr '16*

Providing onsite support for an SCC client, Atradius. Primarily focused on the management of the Windows server estate.
Atradius is a global financial institution specialising in credit insurance. The company has over four thousand users with over 160 offices in over 60 countries and growing with countless external customers and with on premise data centres. Key achievements & responsibilities included;

- Manage & support VMware vSphere clusters
- Introduced Windows server images used to provision both virtual & physical machines leveraging SCCM, significantly reducing the lead time
- Standardised server image reducing the storage footprint by half and incorporating baseline apps
- Assist in the management and support of the Citrix XenApp 6.5 environment
- Represented SCC the customer weekly knowledge team & change approval board in an advisory capacity

PERSONAL SKILLS

- Results driven, forward thinking with a logical problem-solving positive mentality
- Accepts responsibility
- Thrives and excels in owning & leadership roles
- Comfortable working in rapidly changing & evolving environments
- Open minded, easily absorb and digest new strategies, approaches & guidance
- Focus on continuously adding business value

In my spare time I continue to push myself and grow;
Soft Skills: I continue to adapt, grow and learn new skills and practices to introduce into the working day e.g. making stand-up and retrospectives more engaging and valuable.

Technically: I continue and eager to learn new features of dotnet core and Go through creating applications and services that I publish on Github.
Ask about my IoT dashcam or lambda-based Keybase Identity Service.

I also enjoy scuba-diving, helicopter flying, cycling, running, reading books such as *The Phoenix Project*, *the Unicorn Project* and next on my list is *Building and scaling high performing technology Organisations*.

CONTACT DETAILS

N: Rhys Evans
T: 07805 595190
E: rhys@rhysevans.co.uk

REFERENCES

Available on request

CAREER SUMMARY (extended.)

BioMonde | Bridgend

Reason for leaving: Headhunted by SCC

Systems Administrator *May '14 - Oct '14*

BioMonde is a multinational biomedical manufacturer with offices in the UK, Europe and the USA. BioMonde had no IT strategy and the infrastructure reflected this. Key achievements in the role;

- Global design & implementation of distributed file systems, Active Directory & EUC roaming
- Seamlessly performed an AD cross forest migration on to a new AD forest with no disruption to end users
- Introduced Hyper-V and virtualization for hub/spoke sites

QuickSmart IT | Cardiff

Reason for leaving: Left to pursue opportunities working for a international company

Technical Lead & *March '13 - April '14*

3rd Line Support Engineer

LANSecure IT | Cardiff

Reason for leaving: Made redundant

3rd Line Support / Consultant *Sept '10 - Jan '13*

1st / 2nd Line Support *Sept '09 - Aug '10*