**Thomas Munn**

|  |  |  |
| --- | --- | --- |
| Cary, NC 27513 | 919-648-2447 | [thomas.j.munn@icloud.com](mailto:thomas.j.munn@icloud.com) |

**Principal Cloud Security Engineer**

*Cloud Security, Container Security, Analytics & Compliance, IOT Design and Audit*

I have helped companies attack modern Kubernetes container problems in AWS. I bring an out-of-the-box creative and technically sound perspective to my clients. I serve as their guide, explaining difficult technical problems clearly. I help them make the best choices based upon their needs. All container technologies should be secure and safe. They should help businesses bring secure solutions to their clients. Customers’ data needs to be private and still usable, within an increasingly complex international regulatory environment. I value an open mind, since it is the key to good relationships with my colleagues and clients.

***Areas of Expertise***

|  |  |
| --- | --- |
| *Focus Areas* | *Skill Areas* |
| * Analyzing risk tolerance vs cost in IOT and Container solutions * Imparting innovative SecDevOps culture * Solving tough security problems unconventionally * Forensics & Incident Response | * Secure Pipeline and Container designs * Sensible PKI / Usable PKI Solutions * Creatively balancing security vs utility * Vendor agnostic Kubernetes and Docker solutions |

***Technical***

* OS and Languages: OpenWRT, Windows server 2016, FreeBSD, Linux Variants (RedHat, Debian), TwistLock, Bash, Ansible, PowerShell, Kubernetes (version 1.12) bare metal
* Cloud Technology: Amazon Web Services, Azure Ad infrastructure, Azure Sphere, Kubernetes, Docker, Prometheus, Vagrant, ElasticSearch, Kibana, Notary, Kubernetes
* IOT: OpenWrt, Arm Processors, Secure Boot, Image Provenance, Docker, Linux Containers, PKI
* Technologies: Ansible, Palo Alto, Gitlab, OpenScap, Azure Sphere, Active Directory 2fa, PrimeKey PKI appliance, TrustZone, TPM 2.0, Intel TXT, Selinux, Secure Boot, Trusted Boot, Artifactory, TerraForm, Imperva Waf, F5 ASM Waf

***Professional Experience***

**Xylem Inc, Durham, North Carolina May 2018—Present**

***Senior SecDevOps Engineer***   
Secured Amazon Web Services accounts for meter billing applications. This included installing twistlock, performing network analysis, developing secure VPN / management domain, developing secure container pipeline, as well as advising on GDPR compliance.

*Selected Achievements:*

* **Installed and configured a twistlock secure pipeline for container management and trust provenance within a Kubernetes cluster. This enabled my client to see at a glance which container images had vulnerabilities, and how to remediate them. It also integrated with the Jenkins pipeline to scan images are they came off the pipeline. I helped them to achieve a complete vulnerability life-cycle.**
* Developed prototype secure management domain model for amazon web services including secure VPN access, and secure access to multiple accounts using native Aws features (vpc peering and route53).
* Analyzed VPC flow logs to help tie down any/any access control lists and security groups.

**Cree Incorporated, Durham, North Carolina July 2016 to May 2018**

***Principal IOT Security Researcher***   
Develop new IOT security product. This included cloud, on-prem, and device security. Also developed secure development pipeline for device and cloud asset updating, and developed a signed OpenWrt image for final release to manufacturing. Evaluated multiple IOT infrastructure (ThingWorx, Microsoft Azure IOT, Renesys) platforms.

*Selected Achievements:*

* Crafted a hybrid IOT infrastructure that delivered micro-services to customers. The solution including research, documentation, testing, and final deployment including the development of a custom Secure RedHat OS on Hyper-V. This served as the template for final VM introduction to the Azure Marketplace. Combined both Unix (Ansible) and Windows (azure cli) tools to automate this process.
* Developed secure PKI implementation which combined security with functionality. We used RSA keys with a hardware anchor of trust to make security based upon physical characteristics of IOT devices. This made data opaque to adversaries, and complied with local and international laws.

**SAS, Cary, North Carolina Dec 2015 to May 2016**

***Senior Security Architect***   
Provide security architectural, design and development expertise for SAS startup developing a Big Data security analytics platform.

*Selected Achievements:*

* Defined the target architecture, roadmap and principles for client solution deployments.
* Full life cycle solution delivery and executive advisory. This includes strategy, roadmap, assessments and discovery, design, architecture and solution delivery.

**Verizon, Cary, North Carolina July 2008 to Dec 2015**

***Principal Security Consultant***   
Designed and implemented cloud security solutions. Developed reference architectures. Defined application migration strategies.

*Selected Achievements:*

* Developed and delivered a hybrid cloud solution for a Fortune 100 financial services client using Mashery, IBM Datapower and F5 technologies. Impact: Enabled multi-bank financial transactions for over 10,000 mobile clients.
* Architected, designed and delivered a PCI solution for a Fortune 100 financial client using HPE’s Voltage tokenization platform. Impact: Client passed PCI audit.
* Architected, designed, and delivered a highly resilient EDI platform using IBM API gateway technology. Impact: Enabled a 21.7 billion dollar merger and acquisition of two Fortune 100 financial clients.

***Education and Certifications***

* Bachelor of Science (BS), Information Security, DeVry University, expected graduation 2022
* Certified Information Systems Security Professional (CISSP)
* ITIL V3 certified

***Groups and Associations***

* Active Member – ISC2
* Active Member – Triangle Devops Meetup
* Attended: 2018 Linux Embedded Security Conference