Manager, SOC Architecture, IBM CISO Manager, SOC Architecture, IBM CISO SENIOR MANAGER & CYBERSECURITY LEADER Austin, TX   15 years of experience in Cybersecurity & Enterprise IT   Proven track record of successfully delivering and managing complex enterprise-scale cybersecurity technologies and services   Strategic thinker with ability to build and sustain trusting relationships across enterprise at all levels   Ability to influence across matrixed organization   Adept at managing client, stakeholder, supplier relationships to build organizational synergy   Strong knowledge of application security, network security, and systems security   Experience building scalable architectures for on-prem and cloud environments across large global enterprise   Strong leadership skills - ability to design / drive change   Experience building high-performing Agile teams with top talent - currently managing two teams of 11+ Security Architects and Engineers   Results-oriented - Reputation to always deliver Authorized to work in the US for any employer Work Experience Manager, SOC Architecture, IBM CISO IBM - Austin, TX January 2019 to Present Manage Architecture & Engineering group in IBM CISO SOC. Scope includes SIEM (QRadar), Security Analytics, Data Security (Guardium), Threat Intelligence, Cloud Security, Source Code/IP Protection, Insider Threat, File Integrity Monitoring (TripWire), Incident Response Platform (ServiceNow). Reporting to Executive Director of Enterprise SOC at IBM.   Notable Accomplishments   Scaled and expanded QRadar SIEM on-prem and on Cloud to expand visibility. Current capacity (75 appliances, 900,000 EPS)   Scaled and expanded Guardium deployment on-prem and on Cloud. Current capacity 135 appliances, 200 sensitive and crown-jewel databases boarded   Enabled protection of IBM product source code through user behavioral monitoring of SCMs and Build servers   Developed strategy, business case, and architecture for Threat Intelligence and Threat Hunting programs   Implemented ServiceNow Security Incident Response (SIR) in SOC to enable automation and orchestration; Managed end-to-end engagement with ServiceNow professional services   Evaluated and selected UBA vendor for advanced analytics to detect anomalous events on GitHub access   Responsibilities   Execute global enterprise-scale (multi $M) security deployments to accelerate threat detection and response   Direct and lead development and implementation of security architecture for Security Operations Center   Identify security gaps; Develop business cases with cost/benefit analysis for security spending and initiatives Serve as CISO architectural focal with Business Units and provide consultation on security strategy and recommendations Partner with Business Technology leadership to actively participate in strategic roadmap exercises Ensure GDPR, SOX, FFIEC as well as internal IBM security policy compliance for all services in scope Provide input to corporate security policy team to define policy requirements, standards and controls Interface with security vendors for both procurement and maintenance of security products and services; Provide functional direction to Managed Security Services (MSS) teams for QRadar and Guardium Manage and grow two teams of 11 Security Architects & Engineers; Conduct regular feedback discussions; Support career development; Increase employee engagement and morale through team-building activities Accountable for development and adherence to departmental capital and expense budgets Senior Security Architect & Squad Leader, IBM CISO IBM - Austin, TX January 2016 to December 2018 Responsible for strategy and execution of threat monitoring, security analytics and insider threat programs leading CISO architecture squad and Managed Security Services (MSS) teams. Reported to Exec. Director of SOC & CTO of IBM CISO. Notable Accomplishments Architected and deployed Security Analytics platform for SOC to identify owners of dynamic IP addresses in real-time. Platform uses Big Data technologies such as Hortonworks Data Platform and Elastic stack, processes 30 million events daily, and performs advanced correlation and enrichment in real-time; Used by 150+ users across SOC, CSIRT, Corporate Security Led architecture and implementation of Security Data Lake that provides investigative and proactive threat hunting platform for SOC & CSIRT; Current capacity 500 TB Spearheaded new Data Security shared service leveraging Guardium; Implemented brand new architecture and deployment of Guardium across strategic IBM data centers on-prem and cloud; Established new engagement with external MSSP; Boarded 100+ sensitive and crown-jewel databases for real-time monitoring of unauthorized access Developed new Insider Threat strategy and roadmap for servers and databases.; Led implementation of insider threat use-cases using MITRE ATT&CK Developed logging architecture and SOC monitoring playbook Other Contributions Architecture and deployment of QRadar, Guardium, Security Analytics / Data Lake, ServiceNow, Insider Threat Led integration of CrowdStrike EDR and SignalSciences WAF with QRadar to provide real-time visibility into new threats and attacks to SOC Led Application Security Proof of Concept (POC) with Onapsis to help mitigate risks in SAP system; Responsible for managing all stages of POC: vendor engagement, establishing NDA, organizing internal teams and test environment, developing and executing use-cases and presenting recommendations to leadership Led implementation of an innovative custom DLP/DRM solution using honey tokens for tracking sensitive documents Led development of Corporate Security Log Standard for multiple server OS platforms (Win/AIX/Linux) and Firewalls that provided detailed instructions to enable the logging to adequately captured all relevant security events Performed security assessments and security architecture reviews of large IT environments across IBM Business Units and provided recommendations for security controls Worked closely with FFIEC and SOX project office to ensure compliance; Addressed regulatory requirements for privileged user monitoring; Supported internal/external security audits Completed data privacy assessments for QRadar and Guardium to address EU GDPR requirements Managed vendors and Managed Security Services (MSS) teams; Reviewed and approved SOWs and contracts Led a team of 6 architects and engineers; Responsible for talent recruitment and team development Technical Program Manager, CISO Security Analytics IBM - Austin, TX October 2014 to December 2015 Responsible for strategy and execution of enterprise SIEM QRadar and Resilient Incident Response platform. Notable Accomplishments Spearheaded IBM CISO's first ever global deployment of QRadar SIEM at strategic IBM data centers (NA, EMEA, AP) and oversaw steady state ops Led deployment of Resilient Incident Response Platform to automate CSIRT processes Led delivery transformation from traditional Waterfall to Agile model to improve speed and quality of delivery On-boarded network devices (Cisco ASA firewalls, Bluecoat proxy, Proventia IPS), Linux/AIX/Windows servers, and Symantec endpoint log sources generating 4+ billion events daily Managed supplier relationships, procurement activities, program budget tracking, reporting, and fall planning Multiple Roles: Lead Solution Architect, Technical Project Lead, IT Analyst IBM - New York, NY January 2005 to September 2014 Technical leadership roles in IBM

CIO architecting innovative solutions for engineering info. systems on Java-based platform. Notable Accomplishments Received Outstanding Technical Achievement Award. Implemented and deployed complex Java based solutions for IBM engineering information systems. Addressed issues related to software design, network, database performance. Improved system response time by 5x and system endurance by 30x Directed and supervised multiple development, test, and infrastructure teams across IBM and vendor in a highly matrixed team environment Performed data analysis, scripting, ETL, data modeling, Relational database design and implementation Implemented ITIL best practices and supported security audits and disaster recovery planning Education M.S. in Cybersecurity New York University 2017 M.S. in Information Management Syracuse University 2004 B.S. in Information Systems Stony Brook University 2001 Awards IBM CIO s Outstanding Technical Achievement Award 2014-07 Manager s Choice Awards (multiple) Certifications/Licenses Certified Information Systems Security Professional (CISSP) September 2018 to Present Project Management Professional (PMP) August 2013 to Present Additional Information TECHNICAL SKILLS SIEM QRadar, Splunk Network Security Cisco ASA, Fortinet Fortigate, Palo Alto NGFW, Proventia IPS, Bluecoat Proxy, Cisco VPN, F5 VPN, Wireshark, Nmap, Netcat Application Security Guardium, SignalSciences, Onapsis, Proofpoint, TripWire FIM, OWASP, Burp Suite, Fiddler EDR / AV CrowdStrike, CarbonBlack, Windows Defender ATP, Symantec Penetration Testing Metasploit Big Data Elastic stack, Hortonworks Data Platform (Hadoop, Kafka, Spark, HBase), Apache Nifi UEBA Gurucul, Apache Metron Coding Java, Python, PHP, C, JavaScript, JSP, ASP, Perl, Bash, Qt, JSON, YAML, XML, HTML, CSS, SQL, MQL DevOps Eclipse, GitHub, Travis CI, Rational Team Concert (RTC) Operating Systems Linux (Ubuntu, RHEL, CentOS, Kali, Backtrack), AIX, Unix (Solaris), Windows, Mac Cloud IBM Cloud, AWS S3 Databases Relational (DB2, Oracle, MS Access), NoSQL (Redis, MongoDB) Application Servers Apache Tomcat, Apache HTTP, Websphere Application Server Dashboards / Reporting Kibana, Hyperion, Cognos Performance Testing Rational Performance Tester, HP LoadRunner Regulation/Compliance FFIEC, SOX, GDPR, NIST CSF, RoHS, REACH Others Raspberry Pi 3

Name: James Torres

Email: aduran@example.net

Phone: 983.664.8705