# Ryan Breed

|  |  |
| --- | --- |
| Contact | Info |
| mail | [recruit@breed.org](mailto:recruit@REMOVETHIS.breed.org) |
| voice | [+1 (661) R-BREED-1](tel:+1-661-R-BREED-1) |
| github | github.com/ryanbreed |
| linkedin | linkedin.com/in/ryanbreed |

## Overview

Seasoned security professional with 19 years of deep technical experience in security assessment, penetration testing, security monitoring, incident response, application security, and security architecture. I have a keen interest in practical applications of large-scale data analysis and infrastructure automation to increase organizational resilience to cyber attacks and other major disturbances. I also have practical experience automating Cyber Threat Intelligence sharing and organizing collective security initiatives through cooperative information sharing with public and private sector entities.

## Education

* University of Texas at Austin LBJ School of Public Affairs - Global Policy Studies (2012–2014)
* University of Rochester - Bachelor of Science in Molecular Genetics 1997

## Experience

### Principal, Critical Infrastructure Security

*Electric Reliability Council of Texas (ERCOT)* Nov 2012 - Oct 2016

Individual contributor responsible for engaging business units to develop strategic opportunities for improving grid and market systems while delivering on key security initiatives.

#### Key Responsibilities

* *Senior Incident Responder*: provide investigation and analytical support for critical incidents.
* *Network Defense Hunt Mission*: develop novel analytics for event data. Exploit home-field advantage to degrade adversarial mobility and freedom of action.
* *Intelligence Lead*: prioritize collection and analysis projects. Develop strategic plans for threats to critical grid and market systems.
* *Technology Lead*: Research and implement emerging technologies for application to business and security challenges.
* *External Interface and Advocate*: Perform outreach to public and private sector via ISO/RTO council and DHS CISCP. Engage in public speaking to advocate for electricity sector needs and share information and practices.

#### Major Accomplishments:

* Automated real-time integration of CMDB, IPAM, access control, and vulnerability data into machine-readable representation of entities, applications, business systems, and infrastructure.
* Automated defensive countermeasures. Used model data to safely deploy automated containment, investigation, and other response countermeasures in response to automated threat detection analytics.
* Implemented TAXII endpoint to ingest STIX cyber threat intelligence feeds and propagate indicators to monitoring and control surfaces.
* Developed security testing for Continuous Integration. Used Bamboo to automate Nexpose for vulnerability and baseline assessment. Security findings over a project-specific risk threshold triggered a build failure and intiated response notification chain.
* Developed automated report and security finding distribution. Management reports were automatically updated and reconfigured based on changes to underlying assets and changes in responsible parties.
* Developed Ansible playbooks for CIS benchmarks and Nexpose vulnerabilities. Automated compliance artifact creation and remediation of findings in dev/test environments. Tickets for specific findings were dispatched to responsible parties where human intervention was required.
* Implemented ELK stack for monitoring BroIDS, auditd, RSA Netwitness, and ArcSight ESM/Connector logs. Developed custom logstash plugins to enable event ingest from CMDB and ArcSight.
* Implemented Telegraf, InfluxDB, and Grafana to translate event data into time series domain for tracking metrics and developing new analytics. Collected system telemetry with telegraf to enable performance analysis.
* Developed scenario and training injects for GridEx III. Developed cyber simulator and ChatOps platform for use during exercise play.
* Developed Big Data test bed - deployed DataStax Enterprise Cassandra, Hortonworks Hadoop, Apache Spark, GraphLab, Neo4j, and JupyterHub environments loaded with data from IT, market, and grid systems. Developed proof-of-concept analyses showcasing each technology platform for evaluation by business and IT owners.

### Manager, Critical Infrastructure Security

*Electric Reliability Council of Texas (ERCOT)* Dec 2009 - Nov 2012

Managed a team of 9 security analysts to cover security operations, monitoring, incident response, compliance controls, and security architecture.

##### Key Responsibilities

* Managed departmental budget, including annual and quarterly forecasting. Developed and presented project proposals for cyber security initiatives.
* Provided guidance and oversight in the capital project process to ensure security objectives were incorporated into investment initiatives.
* Lead audit response efforts for cyber security control activities in NERC CIP and SAS70 compliance programs.
* Managed tasking and tracking to remediate findings from audits and other outside assessments.
* Managed employee performance and aligned career development goals with strategic department objectives.
* Developed working threat model for market and grid operations to guide strategic planning.
* Developed, maintained, and exercised Disaster Recovery and Business Continuity plans for cyber security systems.
* Contracted outside penetration tests and assessments to proactively identify and remediate security issues in business and IT systems.
* Lead participation in public/private partnership projects with DOE and DHS.
* Attained SECRET clearance under DHS Private Sector Clearance Program and attended threat briefings as necessary.

##### Major Accomplishments

* Led implementation of DOE ESNM/CRISP pilot site and participated in program development workshops.
* Developed automated security advisory analysis system to triage, score, and dispatch vendor advisories and vulnerability notifications.
* Represented Cybersecurity Department in GridEx II Exercise Play.
* Represented Electricity Subsector in classified threat workshops for IC at DOE INL.

### Lead, Security Operations

*Electric Reliability Council of Texas (ERCOT)* Dec 2005 – Dec 2009

Performed security monitoring, incident response, and investigations.

#### Key Responsibilities

* Infrastructure design and implementation for SIEM, IPS, IDS, Enterprise Forensics, full-content packet capture, web content filtering, and vulnerability management.
* Workflow development for security operations, monitoring, and investigation processes. Developed dashboards, reports, and incident documentation templates. Documented procedures and created reports for compliance controls.
* SIEM content development for automated analysis of security events.
* IDS/IPS signature development to incorporate cyber observables extracted from investigations into real-time monitoring functions.
* Perform forensic analysis of incident artifacts and other digital evidence. Develop incident reports and brief management on findings and recommended response actions.

#### Major Accomplishments

* Deployed 2 major iterations of ArcSight ESM
* Integrated ArcSight ESM with IBM/ISS IPS, Snort NIDS, Tenable Nessus, Windows Events, UNIX/Network/Firewall Syslog, Oracle RDBMS, Microsoft SQL Server and Symantec Antivirus.
* Developed automated analysis tools for decoding malicious javascript extracted from network traffic.
* Developed full-content packet capture and indexing system to extract packet captures indexed on time and IP address.
* Developed management application for BlueCoat site categorization via local policy database.

### Security Consultant

*Unisys* Mar 2003 - Dec 2005

* Performed security assessments, penetration tests, and risk assessments for clients in the Financial Services, Health Care, Manufacturing, and Public sectors.
* Wrote and presented post-engagement reports to clients and provided guidance for addressing findings in line with business objectives.
* Developed labor models and project materials to support pre-sales and standardize engagement delivery across the security practice.
* Developed application penetration test capabilities and assessment framework for other consultants within the practice.
* Directed team activities for large assessments and security infrastructure implementation projects.

### Senior Staff, Security Engineering

*Zurich Global Assets* Jun 2002 – Feb 2003

* Developed Security and Network Operations Center for ZGA infrastructure.
* Acted as ZGA divisional representative at Zurich Financial Services Global Information Technology Services activities.
* Performed security assessments on ZGA and ZFS infrastructure.
* Administered local IDS, Firewall, and UNIX systems.
* Performed local security monitoring.
* Lead global security monitoring team (Dublin, Zurich, Schaumberg, New York, Los Angeles) across ZFS divisions.
* Lead the global PKI implementation team.

### Technical Services Director

*ThruPoint* Oct 1999 – Jun 2002

* Performed security assessment, penetration test, infrastructure design, and infrastructure implementation projects for clients in Financial Services and Media sectors.
* Served as final internal point of escalation for all security consulting technical matters across the company.
* Developed security test lab for use by other security consultants.
* Directed security projects for large engagements.
* Provided staff skills development assistance for other security consultants.

### Security Consultant

*Securities Industry Automation Corporation (SIAC)* Oct 1998 – Sep 1999

* Did first shift firewall operations for Gauntlet firewalls on the internal perimeter networks.
* Performed start-of-day and end-of-day procedures to ensure continuity of operations for second and third shifts.
* Did requirements analysis for business requests and implemented subsequent infrastructure changes.
* Performed UNIX system administration tasks to support maintenance activities
* Participated in Y2K readiness preparations for NYSE security infrastructure.

### Security Consultant

*Interactive Futures* May 1997 – Sep 1998

* Performed security assessments for clients in the Media, Legal, and non-profit sector
* Designed and implemented CheckPoint and Gauntlet firewalls for VAR customers.
* Designed and implemented Sun Solaris/SPARC systems for VAR customers.
* Supported pre-sales discovery and developed written responses to RFP solicitations.

## Certifications

* Completion of Advanced Training - Mercedes AMG Driving Academy
* Leadership Skills for Managers Certificate Program - University of Texas at Austin Professional Development Center
* Advanced SCADA Security - Idaho National Laboratory National SCADA Test Bed
* Certified SCADA Security Architect - Digital Bond, Inc.

## Courses

* Microsoft Windows Security (SANS-505)
* Reverse-engineering Malware (SANS-610)
* PowerShell (SANS-537)
* Identifying and Removing Malware (SANS-537)
* ArcSight ESM 6.5 Security Administrator and Analyst (HPE-00924200)

## Awards

* Team Player Award - ERCOT March 2016
* 1st place Team Autocross - Mercedes AMG Driving Academy June 2015
* Core Value Award for Expertise - ERCOT April 2014
* Team Player Award - ERCOT April 2014
* Exceptional Performer Award - ERCOT January 2014
* Certificate of Recognition: Principal, Critical Infrastructure Security - ERCOT December 2012
* Team Player Award - ERCOT July 2011
* Team Captain and Winning Team - Idaho National Laboratory NSTB Advanced SCADA Security Training November 2008

## Skills

* *Security*: ArcSight ESM/Logger, Bro IDS, McAfee Network Security Platform, Suricata IDS, RSA Security Analytics/Netwitness, Carbon Black Protection (Bit9 Parity), AppLocker, SILK, Netflow, Gigamon
* *DF/IR*: Volatility Framework, plaso/log2timeline, EnCase, F-Response, Carbon Black Response, Soltra Edge, STIX/CybOx/TAXII/OpenIOC, Cuckoo Sandbox, McAfee Advanced Threat Detection
* *Vulnerability Management*: Rapid7 Nexpose, RedSeal, Tenable SecurityCenter, MetaSploit Pro, PhishMe, OpenSCAP, SCAP/OVAL/XCCDF, Scumblr
* *Crypto/Secret Management* HashiCorip Vault, Microsoft Certificate Services, cfssl, OpenSSL, PKCS11, TPM
* *Automation/Management*: packer, Chef, Ansible, Consul, ActiveDirectory Group Policy, Apache ZooKeeper
* *Languages*: Ruby, Python, R, Shell/Bash, PowerShell, Go/golang, Scala, JavaScript
* *Workflow*: JIRA, SharePoint, Confluence, HipChat, rundeck, Stash, Bitbucket, git
* *Testing*: jenkins, TravisCI, Bamboo, selenium, cucumber, rspec, serverspec, brakeman, rubocop, capybara
* *Data Repositories*: MySQL/MariaDB, PostgreSQL, Cassandra, ElasticSearch, InfluxDB, OSISoft PI System
* *ETL/Pipeline*: Apache Kafka, RabbitMQ, Logstash, Pentaho Data Integration, Flume, Sqoop, Avro, Parquet
* *Monitoring/Metrics*: Telegraf, Kapacitor, Zabbix, Nagios, CollectD, DiamonD, StatsD, Graphite, jolokia, jmxtrans
* *Web*: Apache HTTPD, nginx, varnish cache, squid, haproxy, traefik
* *Virtualization*: VMWare ESX, Docker, QEMU, KVM, OpenStack, Vagrant, AWS EC2
* *Analysis/Visualization*: Jupyter, Rstudio, Apache Spark, Tableau, Pig, pandas, scikit-learn, shiny, grafana, kibana
* *Compliance*: NERC CIP, SSAE16, NIST SP800-53, NIST CyberSecurity Framework
* *OS*: CentOS/RHEL 5-7, Windows Server 2008/2012, macOS, OpenBSD, FreeBSD
* *Network*: Cisco IOS, Arista EOS, openvswitch, ISC BIND, AWS Route53, InfoBlox DDI, wireshark
* *Storage*: ceph, minio, OpenStack Swift, AWS S3