|  |  |  |  |
| --- | --- | --- | --- |
| **C. David Lassalle, Jr.** | |  | |
|  | | | |
| dave@superponible.com | www.superponible.com | | github.com/superponible |
|  |  | |  |

**Work Experience**

*Staff Incident Responder, GE Digital*

November 2015 to Present, New Orleans, LA

* Led major incident investigations during on call rotation
* Hunted for compromises on the network and performed analysis
* Drove the implementation of new technologies supporting the CIRT team across the global environment

*Incident Analyst, GE Capital*

December 2012 to November 2015, New Orleans, LA

* Responded to computer security incidents through containment, remediation, and post incident analysis
* Analyzed malware discovered in incidents and shared indicators
* Conducted forensic analysis of system memory and other artifacts including network-centric, host-centric, and log-centric analysis
* Added new features to artifact collection and processing scripts
* Created standard operating procedures for new CIRT team

*Senior Cyber Security Engineer, DM Petroleum Operations Co.*

March 2007 to December 2012, New Orleans, LA

* Primary technical engineer for maintenance, management, and monitoring of most security systems in use
* Led malware and internal incident response investigations
* Conducted network and web assessments and penetration tests
* Wrote security plans and security control tests for NIST SP 800-53
* Improved monitoring and incident response by implementing SIEM
* Performed risk analyses and wrote system security baselines
* Designed and developed C&A control tracking database

*Information Security Engineer II, Raytheon Company*

August 2003 to March 2007, Garland, TX

* Developed C&A for a large system processing multiple levels of data
* Reduced system install and hardening from 2 weeks to 2 days
* Conducted vulnerability assessments to ensure DCID 6/3 compliance
* Presented tests to DAA for system accreditation
* Trained other engineers during transition of project to prime site

**Education**

*Bachelor of Science in Computer Science (Foundation Honors)*

Minor in Mathematics

Texas A&M University, College Station, TX – May 2003

Overall GPA: 4.0

**Certifications**

SANS GREM

SANS GSEC Gold (expired)

SANS GWAPT (expired)

SANS GCWN (expired)

SANS GCFE (expired)

SANS GCFA (expired)

SANS GCIH (expired)

SANS GCIA (expired)

SANS GPEN (expired)

CISSP

**Tools**

OllyDbg

IDA

Cuckoo Sandbox

Volatility

Sleuth Kit

Remnux and SIFT tools

**Languages**

Perl/PHP/Python

Golang

Java

HTML/CSS/Javascript

C/C++

PowerShell

**Projects**

USNJrnl Parser

Volatility Plugins

srch\_strings\_wrap

Metasploit nCircle import code

**Awards**

SANS Lethal Forensicator Coins

SANS GIAC Advisory Board

Volatility Plugin Contest Winner

**Publications**

GSEC Gold – Broadcast Encryption