CLINT E. BODUNGEN

Sugarland, Texas • (281) 832-3129
E-Mail: cbodungen@outlook.com

I am a Cyber Security Professional and published author with more than 20 years of experience specializing in vulnerability research, penetration testing, and security product development (exclusive to ICS/SCADA since 2003). I have comprehensive experience in every facet of a cyber security program, from advanced technical development to management, and I'm just as comfortable in front of executives as I am working in the lab.

CORE COMPETENCIES

- **General Cyber-Security:** "0-Day" Vulnerability Research/Discovery • Penetration Testing and Advanced Hacker Methodology and Techniques (OWASP, PTES, OSSTMM) • Social Engineering • Vulnerability Assessments • Broad range of experience with security testing/assessment tools, both industry standard as well as personally developed (e.g. Metasploit, IDA Pro, Burp, Immunity Debugger, Peach Fuzzer, Nessus, etc.) • Threat Intelligence/Analysis • Risk Assessment/Analysis (NIST SP800-30, ISO/IEC 27005) • Security Models and Architecture • Security Controls Integration (e.g. Firewalls, SIEMS, IDS, AWL, etc.) • Organizational Risk Management Programs • Regulatory/Standards Compliance (PCI DSS, NIST SP800-53, NIST SP800-64, ISO 27001, NIST Cyber Security Framework, SOX)

- **ICS/SCADA Security:** ICS/SCADA Specific Protocol, Device, and Application Security/Vulnerabilities and "0-day" Vulnerability Discovery Methods • ICS/SCADA Specific (and safe) SVA/Penetration Testing Methods • Industry Regulatory/Standards Compliance (e.g. ISA99/IEC 62443, NIST SP800-82, API 1164, NERC CIP)

- **IT/Networking:** TCP/IP Network Programming/Application Development • Advanced Understanding, Application, and Analysis of TCP/IP Protocols • Experience with Multiple Network Devices/Manufacturers and Network Management Tools • Expert Understanding of Network Architecture/Design

- **Programming:** C/C++/C# • x86 Assembly • Perl • Python • Ruby • Linux Shell Scripting • JavaScript • PHP • Unity3D

PROFESSIONAL EXPERIENCE

- **Derezzed Inc. (dba ThreatGEN) – Houston, TX** **June 2017 – Present**
  CO-FOUNDER/CHAIRMAN & CEO
  - Using computer gaming engines and technology to create creative, bleeding-edge ICS cybersecurity training solutions
  - Original creator and developer of the ThreatGEN ICS Cyber Range Simulation Platform
  - Co-creator and developer ThreatGEN Red vs. Blue Cybersecurity Training Game
  - Creator and lead instructor of the ThreatGEN Red vs. Blue ICS Cybersecurity training course
  - As Chairman & CEO, I'm responsible for creating and driving the company vision and strategy as well as acting as the company spokesman, building partnerships, and building/growing the business in general

- **LEO Cyber Security – Houston, TX** **October 2017 – Present**
  EXECUTITVE VICE PRESIDENT, ICS CYBER SECURITY RESEARCH
  - Responsible for providing pre-sales support, act as key ICS cybersecurity subject matter expert (SME), and provide public thought leadership
  - Responsible for building a world-class ICS Cyber Security business practice, directing the vision and philosophy of the practice, establishing great strategic partnerships and relationships, identifying technological and strategic opportunities, and hiring the most skilled and experienced staff in the industry

- **Kaspersky Lab, North America – Houston, TX** **May 2016 – September 2017**
  SENIOR RESEARCHER, CRITICAL INFRASTRUCTURE THREAT ANALYSIS
  - Principle technical industrial control systems (ICS) Subject Matter Expert (SME) for Kaspersky globally
  - Expanded Kaspersky brand awareness and credibility within the North American ICS market
  - Researched and analyzed current and emerging ICS threats and vulnerabilities
  - Coordinated vulnerability disclosure with vendors and DHS ICS-CERT
  - Provided content for and approved ICS related media releases
  - Interfaced with the media for ICS related interviews
  - Researched and developed industry leading, cutting edge applications, tools, and technology for industrial control systems
  - Author of Kaspersky Lab's ICS Penetration Testing Training Course
  - Presented at several industry conferences as an ICS subject matter expert and evangelist
  - Instructor and presenter at multiple ICS cybersecurity workshops at MIT (Massachusetts Institute of Technology)

- **Booz Allen Hamilton – Houston, TX** **February 2015 – May 2016**
  SENIOR INDUSTRIAL CYBERSECURITY ANALYST/RESEARCHER
  - Lead and performed ICS security risk assessments and penetration testing projects
  - Lead architect of the Probabilistic Risk Assessment Model (PRAM)
  - Subject Matter Expert (SME) and technical developer for Booz Allen Hamilton's ICS security predictive analytics
  - ICS security SME for risk assessment and penetration testing related marketing efforts, business development, proposals and projects
  - Developed multiple whitepapers and presented at several industry conferences.

- **Cimation – Houston, TX** **July 2013 – January 2015**
  R&D MANAGER, CYBER SECURITY SOLUTIONS
  SENIOR ICS/SCADA SECURITY RESEARCHER
  - Performed ICS/SCADA "0-day" vulnerability research/discovery, malware analysis, intrusion detection system (IDS) signature development, proof of concept (POC) code and exploit development, penetration testing, and vulnerability assessments.
  - Performed the research & development of cutting edge and innovative ICS security technologies/solutions and penetration testing/vulnerability research tools using the Agile Product Development Life-Cycle.
  - Principal Architect and developer of Cimation's threat intelligence and vulnerability feed online interface.
  - Program architect, principal course developer, and lead instructor for Cimation's online ICS/SCADA cyber security training program and Cimation University (online ICS/SCADA security training).
  - Principal contributor to Cimation's vulnerability research and threat intelligence program business model and strategic roadmap.
  - Key contributor to the creation and documentation of Cimation's security services program and services catalog.
  - Principal contributor to Cimation's vulnerability assessment and penetration testing standard operating procedures, processes, and methodologies.
  - Provided support for business development, sales, and marketing as a subject matter expert.
  - Developed multiple whitepapers and presented at several industry conferences.

- **CIDG Corp./Amor Group, LLC. (A Lockheed Martin Company) – Houston, TX** **January 2008 – July 2013**
  CIDG FOUNDER
  AMOR GROUP SENIOR SECURITY CONSULTANT/ANALYST
  - Co-founder of CiSACS (Comprehensive Industrial Security and Compliance Solution).
  - Performed cyber, physical, and operational Security Vulnerability Assessments (SVA), penetration testing, "red team" testing, risk assessments, and regulatory compliance assessments (gap analysis) for ICS/SCADA environments as team lead/project manager.
  - Assisted clients with building and maintaining ICS/SCADA Security and Risk Management programs.
  - Recommended and deployed risk mitigation strategies and technologies (including SIEM technology).
  - Responsible for business development and sales support for vendor technologies.
  - Published multiple whitepapers on ICS/SCADA Security.
  - Maintained the security lab for threat analysis, vulnerability/exploit research, technology/product evaluation, and training.
  - Presented at multiple industry conferences.

- **Plantdata Technologies/Industrial Defender – Houston, TX** **November 2004 – January 2008**
  SENIOR SECURITY CONSULTANT
  - Developed security auditing tools and testing standardization across the company's security consulting services.
  - Performed penetration testing, risk/vulnerability assessments, recommended and implemented mitigation strategies, designed and implemented security policies for the some of the world's leading and largest energy, utility, oil & gas, and communication companies.
  - Tested the Emerson DeltaV Controllers for security vulnerabilities on-site at Emerson.
  - Presented at multiple industry conferences.

- **Critical Infrastructure Institute (CII) – Houston, TX** **November 2004 – January 2008**
  CO-FOUNDER AND PRESIDENT
  - Creator of the PCIP (Professional in Critical Infrastructure Protection) concept and certification program.
  - Maintained the PCIP Technical Course material.
  - Taught the PCIP certification course in the U.S. and Canada.
  - Developed business and media relationships expanding CII to an international organization with training centers in the US, Canada, Italy, Romania, Singapore, and the UK.
  - Presented at multiple industry conferences.

- **Diverse Networks – Houston, TX** **November 2003 – November 2004**
  SCADA SECURITY CONSULTANT

- Performed penetration testing, risk/vulnerability assessments, recommended and implemented mitigation strategies, designed and implemented security policies for the some of the world's leading and largest energy, utility, oil & gas, and communication companies.
- Implemented security mitigation and remediation for Chevron-Texaco's RTAP SCADA systems.
- Developed a secure, remote, wireless alarm solution for controllers on the SCADA network for Chevron-Texaco Pipeline.

- **First Community Bancshares, Inc. – Killeen, TX** **August 2002 – November 2003**
  (1st National Bank Texas, 1st Convenience Bank Texas, Fort Hood National Bank, and 1st Community Services)
  VICE PRESIDENT, IT SECURITY AND DISASTER RECOVERY
  CHAIRMAN, DISASTER RECOVERY COMMITTEE
  - Built and managed the IT Security team responsible for IT Security maintenance, administration, and testing enterprise-wide for over 200 bank branches.
  - Developed and managed department budget, cost/benefit analysis, policies, procedures, and guidelines.
  - Performed enterprise-wide risk analysis and vulnerability assessments.
  - Implemented security controls, vulnerability remediation, and risk mitigation technologies.
  - Developed an "In-House" application/tool specialized in detecting unique viruses/worms designed to evade IDS and Anti-Virus preventing major virus risks such as the Bugbear.b.
  - Renegotiated the Disaster Recovery contract, with a new vendor, increasing recovery capabilities and saving the company $1.7 million a year.

- **Symantec Corporation (6-month Contract) – San Antonio, TX** **February 2002 – August 2002**
  NETWORK INTRUSION DETECTION SYSTEMS DEVELOPER – SQA ENGINEER
  - Developed IDS (Intrusion Detection System) software and quality assurance tests.
  - Developed attack signatures for the Symantec Net Prowler IDS.
  - Performed Net Prowler IDS sustainment and attack signature update quality assurance testing.
  - Taught the CISSP (Certified Information Systems Security Professional) preparation course to Symantec employees.
  - Configured lab systems and networks to accommodate testing environments, which included simulating attacks/intrusions as well as securing and "hardening" each environment for proper IDS testing.

- **SynchroNet, Inc. – Houston, TX** **October 1999 – February 2002**
  VICE PRESIDENT, SECURITY OPERATIONS
  - Helped build the Information Security Department from the ground up to include research and development of technologies, hiring and training personnel, and establishing policies and procedures.
  - Engineered and Implemented network security solutions for corporate and private clients across the United States utilizing multiple vendors and systems.
  - Performed firewall development and installation, risk analysis, vulnerability assessments, penetration testing, intrusion detection systems development and implementation, policy/procedure design, custom security software development, and client education.
  - Engineered and developed a proprietary packet filtering firewall, VPN, and IDS network appliance with a web-based configuration interface that was deployed on several client sites.
  - Developed an innovative patch for Betrieve (A common database Engine) that resolved a multi-user connectivity issue between Peachtree Accounting, Citrix Metaframe, and Betrieve. The issue was resolved by reprogramming the MKDE (Micro-kernel Database Engine) file and 2 data link libraries in hexadecimal code.

- **United States Air Force – Barksdale AFB, LA** **April 1995 – October 1999**
  PRIMARY AFSC: 2T231 – AIR TRANSPORTATION JOURNEYMAN
  ADDITIONAL ASSIGMENT: COMPUTER SYSTEMS SECURITY OFFICER/OPSEC MANAGER
  - Developed disaster recovery/contingency plans, information security policies, and training procedures for local base regulations and while deployed to Diego Garcia for Operation Desert Strike.
  - Performed risk analysis, vulnerability assessments, and penetration tests base-wide during regular contingency exercises, Operation Southern Watch (Saudi Arabia), and Operation Desert Strike (Diego Garcia B.I.O.T.)
  - Maintained accountability and security for systems and software at both squadron and wing level to ensure maximum information and network security.
  - Worked with other government organizations on computer crime related investigations.

EDUCATION & CERTIFICATIONS

- Course completed. OSCP (Offensive-Security Certified Professional), have not yet tested for certification
- Course Completed: GICSP (Global Industrial Cyber Security Professional), have not tested for certification
- Certification: PCIP (Professional in Critical Infrastructure Protection)
- Course Completed: CCNA (Cisco Certified Network Associate)
- Certification: Webthority (Web Security Software)
- Certification: Enterprise Security Manager and Intruder Alert (Intrusion Detection Software)
- Certification: Advanced Network Security
- Certification: Computer Programming (National Radio Institute)

- **Colorado Institute of Art – Denver, CO** **1993 – 1995**
  Degree: Associates, Industrial Design Technology

- **Game Institute** **2014 – Present**
  Game Design and Programming (No Degree Earned)
  Courses:
  - *C#/C++ Programming*
  - *Unity3D*
  - *Artificial Intelligence*
  - *Mathematics for Gaming Physics*
  - *Electronics & Robotics*
  - *3D Graphics & Game Engine Programming*
  - *3D Art & Animation*

- **Louisiana Tech University – Barksdale AFB, LA** **1997 – 1999**
  Course of Study: Computer Science (No Degree Earned)

- **Community College of the Air Force – Barksdale AFB, LA** **1997 – 1999**
  Course of Study: Information Technology/Computer Science (No Degree Earned)

INDUSTRY RECOGNITION AND EXPOSURE

- **Conferences Presented At:**

  - **RSA, Hou.Sec.Con, SANS ICS Summit, S4, UtiliSec, PCSF/ICSJWG, API, INTELEC, CyberShield, ShaleComm, OilComm, ICS Cybersecurity Conference, Public Safety Canada Safety & Security Symposium, ISA Cybersecurity Summit**

- **Publications:**

  - **"Hacking Exposed: Industrial Control Systems - ICS/SCADA Security Secrets & Solutions"**
    Book – McGraw Hill – September 2016
  - **"Penetration Testing & Other Cyber Security Buzzwords: What Companies Really Need to Know"**
    Blog Post – LinkedIn.com (https://goo.gl/h7NP7E) – January 2015
  - **"Crossing the Great Divide: Bridging the Gap Between Enterprise and Industrial IT"**
    Whitepaper – Cimation.com – April 2014
  - **"Set it and Forget it: The Automation of Hacking"**
    Blog – Cimation.com – September 2013
  - **"Introduction to SCADA Security"**
    Online Lecture – Designnews.com – 2013
  - **"The Art of SCADA War: An Owner/Operator's Guide to Pragmatic Process Control Security"**
    Whitepaper – Amor Group/Lockheed Martin – 2012
  - **"SCADA Security, Compliance, and Liability: A Survival Guide"**
    Article and Print – Pipelineandgasjournal.com, Amazon.com – 2009
  - **"Anatomy of a Red Team Attack"**
    Article (Online and Print) – Automationworld.com – 2007
  - **"Watch Out for Bluetooth Hacking"**
    Article (Online and Print) – Automationworld.com – 2007

PERSONAL/INDEPENDENT PROJECTS AT: SECURINGICS.COM