Jesse Trucks jesse@cyberius.net

+1-608-347-3833

SUMMARY OF SKILLS

Security:	GCUX & GCIA certified, incident handling, auditing, servers, networking, firewalls, intrusion detection and prevention, event correlation, policy drafting, authentication, encryption, vulnerability analysis and scanning, log and machine data analytics, unix/linux host defense and detection
Operating Systems:	Senior Unix Systems Administrator (SAGE IV), Sun Solaris, Linux (Debian, Ubuntu, Red Hat Enterprise Linux (RHEL), SUSE), OpenBSD, OS X (Client, Server), Microsoft Windows
Software/Hardware:	DNS, email (Courier, POP, IMAP, SMTP, Sendmail, Postfix, Exchange), Sun Enterprise hardware, MySQL, Apache, LAMP, monitoring, Veritas, enterprise storage, supercomputers (Anton, Cray), Tenable Security Center, Nessus, Snort, Splunk, Sourcefire, Stealthwatch, Solera, BlueCoat, Mandiant Intelligent Response (MIR)
Programming:	Unix shell (sh, ksh, bash), Perl, PHP
Administrative:	Policy development, training, personnel management, customer service, presentations, budgeting, project management, change management, disaster recovery, data center management

EXPERIENCE

PEAK HOSTING **Knoxville, TN**

Director of Security and Compliance **8/2014 – Present**

- Manage Security and Compliance teams
- Design, implement, and maintain various compliance programs
- Build defensive and offensive security capabilities
- Oversee or directly perform incident response and handling
- System and network forensics
- Security data analytics
- Leverage Splunk and other tools for security and risk management

Engineering Director **5/2014 – 8/2014**

- Manage Engineering Department
- Provide strategic direction for Engineering Department
- Assist Network, Software, and Systems Engineering Managers with tactical implementation
- Directly manage Security Engineering team
- Build defensive and offensive security capabilities
- Oversee or directly perform incident response and handling
- System and network forensics
- Security data analytics
- Leverage Splunk and other tools for security and risk management

Jesse Trucks jesse@cyberius.net
+1-608-347-3833

Security Engineering Manager **3/2014 – 5/2014**
(also acting Systems and Software Engineering Managers)
- Manage Security Engineering Team
- Design, implement, and maintain security monitoring and management infrastructure
- Incident response
- Training and mentoring security engineers
- Security related data analytics

Senior Systems Engineer **1/2014 – 3/2014**
- Research, design, and implement distributed systems infrastructure
- Design, implement, and maintain infrastructure automation

OAK RIDGE NATIONAL LABORATORY (ORNL) **Oak Ridge, TN**
Cyber Security Engineer and Team Lead **8/2012 – 01/2014**
Additional duties as listed under HPC Cyber Security Administrator below
- Technical and project lead for Cyber Security Operations and Integration Team
- Splunk and logging infrastructure design, implementation, and management
- Security data analytics and operational intelligence analysis

HPC Cyber Security Administrator **12/2010 – 8/2012**
- Security policy and procedure development, management, and enforcement
- Consult on security aspects of projects and infrastructure
- Build and maintain security management tools, e.g. IDS, file integrity, and monitoring
- Provide technical support and architecture design for security related solutions
- Design, develop, and implement automation processes and applications
- Research and development on supercomputer and cluster security and monitoring systems
- Security incident handling and response

CYBERIUS' NETWORK, Secure and Reliable Systems Consulting **Knoxville, TN**
Sole Proprietor (part-time, independent consulting) **8/1996 – 12/2010**
- Analyzed and evaluated network security systems
- Rebuilt compromised systems and networks
- Assisted clients with technical infrastructure management
- Built and maintained servers (Debian, OpenBSD, OS X, Ubuntu)
- Provided technical support and architecture design for client/server solutions
- Built custom applications and web sites using PHP, Perl and/or MySQL

D. E. SHAW RESEARCH, LLC, A computational biochemistry research laboratory **Endicott, NY**
Systems Engineer **3/2009 – 10/2010**
- Oversaw daily data center operations, such as cooling and power
- Supervised installation and bring-up of 16 Anton supercomputers
- Managed daily production supercomputer and cluster operations
- Supported Rocks HPC Linux clusters
- Developed and maintained policy, process, and procedure documentation
- Designed and implemented internal live training sessions and manuals
- Configured and installed routers, switches, and other networking equipment
- Wrote and maintained internal applications using PHP, Perl, sh/ksh, and/or MySQL

Jesse Trucks

jesse@cyberius.net

+1-608-347-3833

TDS TELECOM, Telecommunications provider — **Madison, WI**

Systems Engineer — **7/2007 – 12/2008**

- Researched and developed technical solutions
- Generated and maintained system, process, and procedure documentation
- Deployed and managed Solaris and Red Hat Enterprise Linux (RHEL) servers
- Designed, managed, and implemented medium to large scale technical projects
- Performed internal Veritas product technical support as subject matter expert (SME)
- Veritas Cluster Server management and design
- Automated reports and processes using shell scripts, Perl, Oracle, and/or MySQL
- Provided advanced technical support to Operational Support team
- Designed and managed server and network architectures
- Supported systems for Oracle, MySQL and MS-SQL RDBMS

IT CONVERGENCE, Oracle solutions, managed services and hosting provider — **Madison, WI**

Technical Services Supervisor — **10/2006 – 5/2007**

- Recruited and developed Systems Administration Team
- Managed U.S. Systems Administration Team
- Maintained Unix, Linux, and Windows systems for multiple clients and internal departments
- Developed and maintained practice, policy and procedure documentation
- Installed and upgraded Unix, Linux and Windows servers
- Managed enterprise storage (SAN, NAS, EMC, iSCSI)
- Administered enterprise backups (NetWorker, NetBackup)
- Managed client expectations and needs
- Served as liaison between Project Managers and Systems Administration staff
- Consulted on security issues and incident handling on both internal and client systems
- Maintained system and network monitoring platform using NimBUS
- Developed and maintained task automation using shell scripting and Perl

AT&T SERVICES, INC., Telecommunications provider — **Madison, WI**

Senior Systems Analyst — **10/2000 – 10/2006**

- Lead Security Administrator for an organization with over 5,000 Unix and Linux servers
- Managed organizational Security Team, including project management and coordination
- Developed and managed security policy and procedure documentation and training programs
- Coordinated audits for policy and regulatory compliance, including Sarbanes-Oxley (SOX)
- Designed and implemented process automation using shell scripts and Perl
- Created and delivered reports and presentations for peers and management
- Provided mentoring and training for Unix systems support and Unix security staff
- Responded to security events and incidents as lead technical resource
- Managed and designed Veritas Volume Manager and Cluster Server configurations
- Designed, implemented and managed Disaster Recovery procedures
- Evaluated, designed, tested, recommended, and/or implemented Unix security solutions
- Assisted in security threat identification and patch management for Unix systems
- Managed Solaris Unix and Red Hat Enterprise Linux (RHEL) systems
- Implemented centralized security management and tracking tools
- Evaluated and began implementing a centralized log analysis solution

Jesse Trucks

jesse@cyberius.net

+1-608-347-3833

MADISON NEWSPAPERS, INC., Newspaper Publisher and *madison.com* Host **Madison, WI**
Online Technical Producer **4/1999 – 10/2000**

- Constructed and maintained comprehensive firewall solution
- Maintained Internet publishing systems using: Harris, FreeBSD, Linux, OpenBSD, Solaris
- Researched and developed new products and technologies
- Built database systems for maintaining dynamic workflow and product delivery (MySQL)
- Managed new product and system implementations
- Trained newspaper editors and reporters on Web site content delivery systems
- Created custom system processes for data conversion and product delivery to outside vendors
- Managed Internet connectivity and servers (Red Hat Linux, OpenBSD, FreeBSD, Solaris)
- Trained *madison.com* staff to use Real Media Open Ad Stream ad delivery system

CHAOTIC MEDIA, LLC., Comprehensive Internet-based Solutions **Madison, WI**
Chief Information Officer/Partner **9/1999 – 4/2000**

- Rebuilt compromised networks for security and stability
- Created and maintained e-commerce systems
- Built and managed Internet servers for internal and client use
- Trained clients on network and server maintenance
- Determined hardware/software needs for internal company solutions
- Managed IT policies and processes
- Assisted in corporate strategic planning

GLOBAL DIALOG INTERNET, Internet Provider **Madison, WI**
System Administrator **4/1997 – 3/1999**

Named "Most Valuable Technician" for 1998

- Developed and maintained network and system security infrastructure
- Created and maintained technical policies and procedures
- Improved customer service through customer surveys, staff training and customer contact
- Hired, trained, and managed technicians for dialup and dedicated support positions
- Trained staff and clients on Internet and networking skills and technologies
- Maintained e-commerce applications
- Built and maintained servers and workstations, including DNS, mail, HTTP, NNTP, and FTP
- Maintained 11 city Wide Area Network (WAN) in southeast Wisconsin
- Maintained office telephony system, including programming and troubleshooting
- Managed departmental budget – 25% of company revenue and spending allocations

Jesse Trucks jesse@cyberius.net

+1-608-347-3833

EDUCATION AND CERTIFICATIONS

GIAC Certified Intrusion Analyst (GCIA) (2013-Present)
GIAC Certified Incident Handler (GCIH) (2005-2009)
GIAC Certified UNIX Security Administrator (GCUX–GOLD) (2003-Present)

Cardinal Stritch University
Coursework toward Bachelor of Science in Management (2007 - Present)

University of Wisconsin Colleges, Online Program
Coursework toward Bachelor of Science degree (2001 – 2004)

Navy Electronics Technician A-School Phase I & II (1993 – 1994)

PROFESSIONAL AFFILIATIONS:

League Of Professional System Administrators (LOPSA) Founding Member
LOPSA Board of Directors (2007 - 2013)
LOPSA-East Tennessee Local Chapter Founder and Vice-President
LOPSA-Madison Local Chapter Founder and former President

SANS/GIAC Advisory Board (2007 - Current)
Chair GCUX Advisory Board (10/2004 – 11/2004)
Vice-Chair GCUX Advisory Board (10/2003 – 9/2004)

MILITARY

United States Navy **11/1992 – 5/1994**
Electronics Technician Seaman Apprentice (ETSA)

Jesse Trucks jesse@cyberius.net

+1-608-347-3833

PRESENTATIONS AND TRAINING:

SplunkLive Nashville 2014 Invited Talk Presenter:

- Automating Operational Intelligence

Splunk .conf 2013 Invited Talk Presenter:

- Automating Operational Intelligence: Summary Indexes and Stats

SplunkLive D.C. 2013 Invited Talk Presenter:

- Automating Operational Intelligence

Pellissippi State Community College Gnosis Lecture Series 2013:

- Blitzkrieg Branding

Professional IT Community Conference (PICC) - PICC 2012 Instructor:

- Blitzkrieg Branding
- Introduction to Security for System Administrators

Professional IT Community Conference (PICC) - PICC 2011 Instructor:

- Blitzkrieg Branding

Professional IT Community Conference (PICC) - PICC 2010 Instructor and presenter:

- Introduction to Virtualized Storage Management
- Mentoring: It's for everyone!

Southern California Linux Expo (SCaLE) - SCaLE-U 2009 Instructor:

- Disaster Recovery: Will you survive?
- Introduction to Virtualized Storage Management

Yet Another Perl Conference North America (YAPC::NA) 2008 Instructor:

- System Administrator Master Class

Ohio Linux Festival (OLF) - OLFU 2007 Instructor:

- Disaster Recovery: Will you survive?
- Storage Management: Basic Concepts and Veritas Storage Foundation

LOPSA Sysadmin Days – Cherry Hill 2007 Instructor:

- Change Management: Why suffer the paperwork?
- Communication for IT: A broad spectrum analysis
- Disaster Recovery: Will you survive?
- Advanced Security: A self-assessment study

LOPSA Sysadmin Days – Phoenix 2006 Instructor:

- Change Management: Why suffer the paperwork?
- Communication for IT: A broad spectrum analysis
- Disaster Recovery: Will you survive?
- Advanced Security: A self-assessment study

SANS Local Mentor Instructor:

- SEC-506: Securing Unix/Linux (10/2003 – 1/2004)