Joel Wickham

Cincinnati, Ohio | 513-532-8016 | JWickham7@gmail.com
in www.linkedin.com/in/joelwickham 🌐 www.JoelW.com

Summary

Results-driven Cybersecurity professional with extensive experience in enhancing operations at the enterprise level. Skilled in aligning end-user needs with long-term resolutions to complex challenges. Adept at evaluating and deploying systems aimed at improving quality and efficiency. Expert troubleshooter, continually focused on identifying, isolating, and resolving technical issues. Strong knowledge of security tools and processes, with experience in Security Operations Centers. Proven ability to command and control outages to restore service and provide support and leadership for high-priority incidents. Highly analytical with a track record of success in optimizing processes, managing incidents, and troubleshooting a variety of issues.

Work Experience

Senior Cyber Threat Analyst   2022-08 - Present

Ascensus

- Primary escalation contact for a 24x7 SOC
- Maintain and utilize a threat intelligence platform.
- Conduct security awareness assessments and training for associates.
- Investigate security and operation incidents in and provide timely responses.
- Stay up-to-date with the latest cybersecurity threats and trends.
- Coordinate with external security vendors and assess security risks for new technologies and projects.

Senior Security Operations Analyst   2019-04 - 2022-08

Ascensus

- Promoted to Senior in July 2021
- Respond to security incidents, ranging from small to large, by analyzing and addressing them in a timely manner.
- Analyze phishing emails using various tools and techniques, and run monthly internal phishing campaigns to raise awareness and enhance remediation training.
- Create and maintain security documentation for processes and procedures, ensuring that they meet regulatory requirements and industry best practices.
- Help plan and execute security projects related to Malware Sandbox Analysis, DMARC, Email Gateway, EDR, and TIP, working closely with cross-functional teams to achieve project goals.

Cyber Security Analyst   2018-01 - 2019-04

Western & Southern Financial Group

- Monitor for cyber security events and anomalies using a variety of tools such as BlueCoat, OpenDNS/Umbrella, SEP, CarbonBlack, Exabeam, and QRadar.
- Analyze files, URLs, domains, and emails to determine their legitimacy, using internal tools as well as online resources such as VirusTotal, URLVoid, IPVoid, and Robtex.
- Create and tune rules and reports in QRadar to improve the detection and response capabilities of the system.
- Help plan and execute security projects related to NYDFS, CarbonBlack, Impreva SecureSphere/CounterBreach, Varonis, QRoc, ServiceNow SecOps, and ReliaQuest, collaborating with cross-functional teams to ensure successful project outcomes.
- Provide recommendations for security enhancements to management and senior IT staff, based on the results of security assessments, risk analyses, and other sources of information.
- Research the latest IT security trends and technologies and share findings with colleagues to promote continuous learning and improvement.

Skills

Analytical
- Problem Solving
- Major Incident Management
- Critical Thinking
- Process Optimization

Desktop/Server OS's
- ESXi (VMware), unRAID
- Windows 98-11
- Windows Server 2000-2019
- Ubuntu 10.04-22.04
- CentOS 5-8

Services
- Exchange
- AD(Active Directory), Samba
- IIS, Apache

Security Tools
- ITSM: ServiceNow SecOps, SummitAI
- SIEM: QRadar, LogRhythm, Devo
- Proxy: BlueCoat, ForcePoint, Netskope
- CASB: Netskope
- DNS: OpenDNS/Umbrella
- EDR: Carbon Black, SentinelOne
- UEBA: Exabeam
- Sandbox: VMRay
- TIP: ThreatConnect, Anomali
- Email: IronPort, Mimecast, Abnormal
- Security Awareness: KnowBe4
- Full Packet Capture: Moloch(Arkime)
- MSSP: Symantec, ReliaQuest, Persistent, SecureWorks

Education

University of Cincinnati
Bachelor's Degree (2015)
Information Technology

Certifications

GIAC Certified Intrusion Analyst (GCIA)
Expired: 11/2022

Incident Commander   2015-08 - 2017-10
GE Digital

• Command and control outages to quickly restore service, providing support and leadership for all high-priority incidents.
• Maintain control, ownership, and operational authority of an outage triage during high-pressure situations, leveraging technical skills to work with L2, L3, and L4 resources to develop an incident mitigation and restoration plan, and guiding technical resources to service restoration.
• Actively direct and prioritize all aspects of the high-priority incident bridge line and chat with urgency, ensuring effective resource management and service restoration.
• Ensure timely engagement of essential technical support teams, and provide updates to high-level management, stakeholders, and customers.

System Administrator   2015-02 - 2015-08
Prospera Solutions Group

• Managed 50+ servers and 700+ desktop/laptops for multiple companies, providing IT consulting services that included everything from the server installs to password resets.
• Used tools such as ConnectWise, Continuum, and LogMeIn on a daily basis to monitor, manage, and troubleshoot IT infrastructure and services.
• Interacted with HP, Dell, Microsoft, and ISP representatives on a daily basis, to ensure timely and effective resolution of IT-related issues.

IT Co-op   2009-12 - 2014-12
University of Cincinnati

• Ensured the security and operational readiness of multiple computer labs across campus, which contained a total of 400+ computers.
• Troubleshot a variety of hardware and software issues, as well as student and faculty account problems, using tools such as Norton Ghost, Track-It, and others.
• Imaged all lab computers using Norton Ghost between every semester, ensuring that they were up to date and secure.