Chrislo Badenhorst

Durban, RSA

clbadenhorst86@gmail.com

+27 65 978 1053

LinkedIn

As a Principal Consultant in Digital Forensics and Incident Response, I spearhead a team of experts in managing and resolving cyber security incidents, conducting forensic investigations, and enhancing organizational security postures. My role encompasses the development and execution of incident response plans, coordination of effective breach responses, and the strategic management of communication and reporting. I possess a profound knowledge of digital forensics, incident response protocols, and the latest cybersecurity trends, coupled with robust leadership and communication abilities to steer critical initiatives and ensure adherence to legal and regulatory standards.

EXPERTISE

Digital Forensics Specialist: Skilled in conducting detailed investigations and analysis of digital evidence to support legal proceedings and incident response strategies. Proficient in utilizing advanced forensic tools and techniques to uncover cyber-crime activities and mitigate security breaches effectively.
Risk Management and Compliance: Expertise in identifying and mitigating risks associated with digital assets and cyber incidents. Demonstrated ability to develop and implement compliance strategies aligned with regulatory requirements and industry standards, ensuring data integrity and confidentiality.
Incident Response Leadership: Experienced in leading incident response efforts to manage and mitigate the impact of security breaches and cyber incidents. Capable of coordinating cross-functional teams to preserve evidence and restore operational integrity promptly.
Professional Development: Actively participates in webinars and industry events to stay updated on the latest digital forensics techniques, cyber threats, and best practices. Committed to continuous learning and professional growth to enhance my skills and adapt to evolving cybersecurity challenges.

CERTIFICATIONS

Hands-on Malicious Script Analysis for Ransomware Response	SANS	2023
SANS DFIR Summit & Training	SANS	2023
Windows Forensics Examiner Course	IACIS	2023
SOC 2 Implementer	Scytale	2023
SANS Ransomware Summit	SANS	2023
CCFE	INFOSEC	2022
(ISC)² CISSP-ISSAP Fundamentals	INFOSEC	2022

EXPERIENCE

Principal Consultant – Digital Forensics and Incident Response, *DF-Labs* **April 2024 – Present**

- Directed the development and implementation of comprehensive incident response plans.
- Led the coordination of swift and effective response efforts during security breaches.
- Managed the strategic communication and detailed reporting processes throughout and following incidents.
- Conducted thorough forensic investigations to assess the scope and impact of security incidents.
- Methodically collected, analyzed, and preserved digital evidence for legal defensibility.
- Skillfully identified the methods and sources of attacks, including sophisticated malware analysis.
- Analyzed threat intelligence to proactively identify potential security risks.
- Conducted in-depth risk assessments to evaluate and address organizational vulnerabilities.
- Proactively provided recommendations to mitigate identified risks and enhance security posture.
- Advised organizations authoritatively on best practices for security and compliance.
- Guided the implementation of robust security controls and policies expertly.
- Assisted diligently with the development of security awareness and training programs.
- Ensured meticulously that digital forensics and incident response activities complied with relevant laws and regulations.
- Supported efficiently the preparation for and response to regulatory inquiries or audits.
- Stayed abreast of cutting-edge technologies, tools, and techniques in digital forensics and incident response.
- Mentored team members effectively, providing technical leadership and fostering professional growth.
- Contributed significantly to the development of innovative forensic tools and methodologies.
- Cultivated and maintained strong relationships with clients, understanding their needs and delivering tailored solutions.
- Played a pivotal role in identifying new business opportunities and contributed substantially to proposal development.
- Prepared detailed and compelling forensic reports, presenting complex findings clearly to stakeholders.
- Documented incident response activities meticulously, maintaining accurate and comprehensive records.
- Assisted in the creation of educational materials and whitepapers, sharing knowledge and insights widely.
- Prepared for and delivered expert testimony in legal proceedings with confidence, collaborating closely with legal teams.
- Reviewed and enhanced incident response processes and procedures continuously.
- Contributed to the ongoing enhancement of digital forensics capabilities within the organization.
- Encouraged a culture of continuous learning and improvement within the team, setting high standards for excellence

Principal Consultant, Secure Sphere Consulting **July 2023 - March 2024**

Cyber Security Advisory

- Directed the strategic planning and implementation of robust cybersecurity programs.
- Led comprehensive cyber risk assessments and advised on enhancements to security posture.
- Developed and executed breach and attack simulations to fortify security defenses.
- Managed vulnerability management processes, ensuring timely identification and remediation of weaknesses.
- Contributed to pre-sales efforts by crafting tailored cybersecurity solutions and proposals.
- Spearheaded incident response and management activities, guiding teams through containment, eradication, and recovery.
- Mentored cybersecurity professionals, fostering a culture of expertise and continuous improvement.

Cyber Security Analyst

- Vigilantly monitored and analyzed security alerts, swiftly investigating potential breaches.
- Proactively utilized security tools to detect and prevent threats, conducting regular assessments.
- Meticulously documented and reported security findings, recommending actionable improvements

Breach and Attack Simulation Specialist

- Expertly simulated cyber-attacks to uncover vulnerabilities and test security controls.
- Collaboratively worked with teams to enhance incident response capabilities.
- Articulately presented detailed reports, proposing targeted mitigation strategies.

Vulnerability Management Expert

- Efficiently identified and classified vulnerabilities, prioritizing based on risk impact.
- Coordinated seamlessly with IT staff for prompt and effective patch management.

Pre-sales Cybersecurity Advisor

- Engaged closely with the sales team to align cybersecurity offerings with client needs.
- Creatively designed and delivered compelling presentations that showcased cybersecurity solutions.
- Cultivated strong relationships with prospective clients, understanding their unique security challenges.

Incident Response Manager

- Decisively led incident response efforts, orchestrating teams to address security incidents.
- Ensured clear communication with stakeholders, navigating complex post-incident landscapes.
- Conducted thorough post-mortem analyses, refining response protocols for future incidents.

Solutions Architect, *Risk X* **Oct 2021 - June 2023**

- Strategically designed and implemented innovative technology solutions that aligned with business objectives and enhanced operational efficiency.
- Collaborated closely with cross-functional teams to understand complex requirements and translate them into actionable architectural designs.
- Led the development of cloud-based infrastructure, ensuring scalability, reliability, and security.
- Proactively identified and mitigated potential risks and bottlenecks in system architectures.
- Championed the adoption of best practices in software development and integration.
- Mentored junior architects and engineers, fostering a culture of technical excellence and continuous learning.
- Drove the creation of architectural artifacts, including diagrams, documentation, and strategic roadmaps.
- Engaged with stakeholders to communicate architectural decisions and their business implications effectively.
- Continually researched and evaluated emerging technologies to inform future-proof solutions.
- Played a pivotal role in the successful delivery of high-impact projects, contributing to the organization's competitive advantage.

IT Consultant, *Taylor Consulting* **June 2019 - Sept 2021**

- Expertly managed the upkeep, troubleshooting, and enhancement of legacy Access Databases.
- Offered specialized support for resolving issues in applications built with "R."
- Conceived, constructed, and rolled out innovative databases utilizing PHP and MariaDB.
- Orchestrated the seamless transition of outdated Access Databases to contemporary PHP-driven platforms.
- Maintained close collaboration with clients to guarantee that project outcomes met their requirements.
- Spearheaded project scheduling and delivery, ensuring prompt and effective realization of objectives.

IT Manager, *BOSSS Marine Services* **June 2008 – May 2019**

- Meticulously supervised and mentored IT department staff to ensure the seamless and efficient operation of all IT functions.
- Skillfully managed relationships with third-party vendors to optimize service delivery and enhance operational efficiencies.
- Ensured robust and uninterrupted connectivity of LAN/WAN/MPLS networks, underpinning the organization's communication backbone.
- Strategically implemented and maintained comprehensive network security measures to safeguard against cyber threats and data breaches.
- Spearheaded the meticulous planning and execution of IT infrastructure projects, driving innovation and technological advancement.
- Swiftly diagnosed and resolved infrastructure issues with precision, minimizing downtime and maximizing system availability.
- Efficiently administered and installed CRM and PABX systems, ensuring their optimal performance and contribution to business processes.
- Guaranteed the reliability of business-critical applications and facilitated uninterrupted business continuity for voice and data services.
- Integrated ITIL best practices and vigilantly monitored compliance with third-party SLAs to uphold service quality standards.
- Prudently managed IT budgeting to optimize expenditures and maintained optimal network storage solutions for scalability and performance.
- Oversaw the seamless operation of IP networking, network printing, and Wi-Fi services, ensuring accessibility and connectivity throughout the organization.

- Provided comprehensive support for Microsoft Office, Pastel Partner & Payroll, and Microsoft Exchange, enhancing user productivity and efficiency.
- Assisted with the configuration and maintenance of proxy, firewall, and Google Apps ecosystems, fortifying the organization's security posture.
- Implemented and sustained robust backup systems and CCTV surveillance, ensuring data integrity and physical security.
- Managed the network infrastructure with proficiency, including Active Directory and a variety of Windows operating systems, to ensure a stable and secure IT environment.
- Conducted thorough troubleshooting and repairs for desktop and notebook computers, maintaining a high level of system reliability and user satisfaction.
- Crafted and managed impactful digital and vinyl signage, enhancing communication and brand presence within the organization.
- Furnished reliable helpdesk assistance and conducted insightful staff training sessions, empowering users with the necessary IT skills and knowledge.
- Maintained the company website with diligence and supported the installation, setup, and maintenance of various Windows OS versions, ensuring compatibility and functionality across the organization.

Stores Supervisor, *Blinds Mart* Jan 2007 – May 2008

Rooikat Gunner, SANDF Jan 2005 – Dec 2006

CERTIFICATIONS CONTINUED

GO Programming Language	Great Learning	Apr 2023
Incident Response Process	INFOSEC	Dec 2022
Security Operations Architecture	INFOSEC	Nov 2022
Architect for Governance, Compliance and Risk Management	INFOSEC	Nov 2022
Architecture for Application Security	INFOSEC	Nov 2022
IAM Architecture	INFOSEC	Nov 2022
Cyber Solutions Fest 2022 Threat Hunting & Intelligence	SANS	Oct 2022
Foundations of Breach & Attack Simulation	AttackIQ	Feb 2022
Foundations of Operationalizing MITRE ATT&CK	AttackIQ	Feb 2022
Dot NET Web API, Vue JS & Microsoft SQL Full-Stack Web App	Udemy	Jan 2022
R Programming A-Z™ R For Data Science	Udemy	Jan 2022
NDG Linux Unhatch-certificate	Cisco Network Academy	Mar 2020
Microsoft Access Networking 2 - Maximum Security	Udemy	July 2019
Upsize Your MS Access Business Information to MS SQL Server	Udemy	July 2019
Microsoft Access VBA	Udemy	June 2019
Microsoft Access 2016 Master Class	Udemy	May 2019
Access - Networking Made Simple	Udemy	May 2019
ITIL 2011 Foundations	IT Academy	Feb 2016
Windows Server 2008 Network Infrastructure 70-642	IT Academy	July 2013
Windows 7 Configuration 70-680 (MCP)	IT Academy	Apr 2013
CompTIA N+	IT Academy	Feb 2013
CompTIA A+	IT Academy	Feb 2013
Commendation Certificate – Excellent Service Rendered	SANDF	Dec 2005
1SSB - Crew & Troop Training	SANDF	Nov 2005
Certificate of Participation – Ex Seboka	SANDF	Oct 2005
76mm Rooikat Gunnery – Pantserskool	SANDF	July 2005

REFERENCES

References on request.