Gregory Parker
Cybersecurity Analyst

Gregory Parker
20100 Park Row Drive
Katy, TX 77449

(346) 586-3102
parker28gregory@gmail.com

—

Skills

Detail-oriented Cybersecurity Analyst with hands-on experience in threat modeling, incident response planning, system enumeration, and SIEM log analysis (Splunk/Elastic). Leveraging a strong foundation in network configuration, NIST, and MITRE ATT&CK, I transform complex security data into actionable insights. My background in risk assessment, compliance, and investigative analysis strengthens data-driven decision-making. Known for creative problem-solving and critical thinking, I deliver structured analyses that mitigate risk and enhance operational intelligence.

Technical Skills:

Continuous monitoring: SIEM maintenance and use (Splunk, Wazuh); triage and investigation of alerts; writing and

fine-tuning detection rules (SIGMA & YARA); threat modeling using the MITRE ATT&CK matrix; using threat intelligence & OSINT.

DevSecOps: Firewall configuration (pfSense, ModSecurity); vulnerability assessment, exploitation, and remediation.

DFIR: Creating IRPs using NIST CSF; following IR playbooks; testing using tabletop exercises.

Project and Lab Experience

Penetration Testing Report:

● Vulnerability Discovery and Exploitation: Successfully identified and exploited at least one critical vulnerability in the MegaQuagga environment, including a vulnerable WordPress plugin, and potentially discovered additional security weaknesses through comprehensive testing.

● Post-Exploitation Activities: Conducted post-exploitation activities using tools like Metasploit and Meterpreter sessions to demonstrate the impact of discovered vulnerabilities and assess the extent of potential system compromise.

● Formal Penetration Testing Report Creation: Documented all findings, methodologies, and recommendations in a comprehensive penetration testing report following industry standards, including executive

summary, scope definition, methodology documentation, vulnerability details with exploitation steps, and security recommendations for remediation.

Vulnerability Assessment:

● Conducted MegaQuagga Vulnerability Assessment: Performed comprehensive vulnerability scanning using Nessus tools, including both a Basic Network Scan and a Credentialed Patch Audit scan on the Windows Server to identify security weaknesses in the MegaQuagga environment.

● Created Executive Summary and Remediation Documentation: Developed a formal Executive Summary document that communicated vulnerability findings to stakeholders and compiled a detailed Remediation List

spreadsheet outlining specific steps to address discovered vulnerabilities.

● Generated Technical Assessment Reports: Produced HTML reports from the Nessus scans that provided

detailed technical documentation of the vulnerability assessment findings, including the "MegaQuagga VA" basic network scan results and "Windows Server" credentialed patch audit results.

Network Modernization:

● Conducted Comprehensive Threat Modeling Analysis: Performed detailed threat modeling for Xibalba Interactive using structured worksheets to identify potential threat actors, attack vectors, and security vulnerabilities across their gaming platform infrastructure.

● Developed Multi-Stakeholder Security Solutions: Created tailored security recommendations including honeypots, data sources, and mitigations with specific arguments crafted for different stakeholder groups (Executives, IT Teams, and Legal/Compliance) to address identified threats.

● Produced Formal Threat Model Report: Compiled findings into a professional threat modeling report with executive summary, detection strategies, mitigation plans, and SMART goals for implementation, following industry-standard documentation practices for cybersecurity assessments

Experience

Tripleten/ Cybersecurity Analyst
July 2025 - Present, Remote

Engineered SIEM-based detection capabilities (Splunk, Wazuh) using MITRE ATT&CK, improving simulated threat identification accuracy and developing 15+ SIGMA/YARA rules that boosted detection efficiency by 30%.

● Executed incident response simulations and created IRPs aligned with NIST CSF, reducing potential response gaps by 25% through structured escalation and mitigation procedures.

● Analyzed and investigated simulated security alerts across multiple attack vectors, enhancing detection coverage through OSINT, threat intelligence, and ATT&CK-aligned analysis.

Allstate Insurance / Client Risk Advisor
January 2024 - Present, Remote

● Reduced customer exposure to financial and compliance risk by analyzing 100+ client risk profiles

monthly and applying structured assessment frameworks/regulatory controls aligned with data privacy standards.

● Strengthened compliance posture by proactively adapting workflows to regulatory updates by continuously monitoring industry policy and governance changes.

● Improved documentation accuracy and audit readiness by maintaining 98%+ data integrity by implementing structured intake validation and secure data-handling procedures.

Farmers Insurance / Information Risk Relationship
July 2022 - January 2024, Houston, Texas

● Mitigated client financial risk exposure by conducting detailed coverage gap analyses for 50+ accounts monthly by applying structured risk review methodologies.

● Improved audit traceability by maintaining 100% documented account interactions by following secure data-handling best practices.

●Enhanced stakeholder trust and cross-functional alignment by leading structured client review meetings and presenting risk mitigation strategies.

Progressive Insurance / Risk Incident Analyst

July 2021 - July 2024, Houston, Texas

● Investigated and resolved auto claims while maintaining empathy and professionalism

● Explained coverage decisions clearly to customers, ensuring transparency and understanding.

● Collaborated with appraisers, repair shops, and carriers to expedite claim resolutions.

Shell Energy/ NRG Critical Infrastructure Analyst
March 2020 - May 2021, Houston, Texas

● Supervised and trained team members on process adherence, regulatory requirements, and data-handling standards.

● Ensured first-call resolution while properly escalating complex customer issues, similar to security incident escalation models.

●Maintained working knowledge of ERCOT, TDSP , and PUCT regulations, reinforcing compliance-focused operations.

AIG Travel Guard / Risk Assessment Associate
January 2017 - January 2020, Houston, Texas

● Reviewed and validated insurance coverage by following strict internal policies and compliance procedures.

● Handled high volumes of inbound calls involving confidential customer and claims data.

● Collaborated with claims teams to verify eligibility and ensure accurate determinations.

Recognized for high performance while maintaining procedural accuracy and data integrity.

United Recovery Systems / USAA Financial Risk and Security Analysis
December 2015 - January 2017, Houston, Texas

● Negotiated sensitive financial matters while adhering to regulatory and ethical guidelines.

● Trained new hires on compliance requirements and operational procedures.

● Managed high-volume communications while maintaining detailed documentation and accuracy.

Xerox Services / Sprint Customer Care/ Sales Supervisor
February 2014 - December 2015, Houston, Texas

● Trained and supervised new agents on policy adherence, system usage, and data-handling standards.

● Ensured quality assurance through monitoring performance and documentation accuracy.

● Balanced leadership responsibilities with direct customer support in a regulated environment.

Education

Cybersecurity Analyst Certificate | TripleTen | Remote **05/2026**

High School Diploma | Kempner | Sugar Land, TX **06/2011**

Certifications & Projects

CompTIA Security+ **05/2026**

Map and Secure A Network

Update an outdated monolithic network:

https://docs.google.com/presentation/d/17aQrQEeP2vFnSK_9LpSn7ET9Wag-cCTVQBIdfB97Iv4/edit?usp=sharing

- **Assessed and redesigned a legacy enterprise network supporting a mission-critical IBM AS/400 ERP environment, balancing modernization efforts with business continuity and operational constraints.**
- **Developed a secure network architecture by replacing obsolete Token Ring infrastructure with a scalable, resilient Ethernet-based design incorporating network segmentation, redundant connectivity, and high-availability principles.**
- **Performed risk analysis on legacy systems, identifying**

vulnerabilities related to outdated hardware, single points of failure, disaster recovery, remote access, and cybersecurity, while recommending mitigation strategies aligned with business objectives.
- Designed infrastructure improvements including modern routing and switching, secure VPN-enabled remote access, centralized network monitoring, disaster recovery planning, and enhanced internet connectivity to support cloud services and e-commerce initiatives.
- Collaborated with business stakeholders to align technical recommendations with organizational goals, enabling digital transformation, improved operational resilience, enhanced security posture, and readiness for future growth and potential acquisition.

Enumerate network devices using iTop and secure network:

https://drive.google.com/drive/folders/1VZAuQ9XcfjBizmQeZjpoGAisva_qLVCw?usp=sharing

- Conducted comprehensive network enumeration using Nmap and iTop to identify unmanaged assets and discover devices missing from the organization's Configuration Management Database (CMDB).
- Validated and updated CMDB records by comparing scan results against existing asset inventories, identifying discrepancies, and documenting unknown or unauthorized devices for remediation.
- Performed traceroute analysis and interpreted network topology to map asset locations, verify routing paths between LAN, DMZ, and WAN segments, and improve infrastructure documentation.
- Created and maintained accurate asset documentation by correlating hostnames, IP addresses, operating systems, and network roles, strengthening asset visibility and supporting incident response readiness.
- Documented network findings, unresolved asset discrepancies, and recommended CMDB updates to establish a reliable source of truth, improving security operations and adherence to cybersecurity best practices.

Security Posture Analysis:

https://drive.google.com/drive/folders/1m_n0ZY1p-MAyxTuZ2Lix2C0C0uf8Nxo3?usp=drive_link

- Analyzed a ransomware incident case file to identify security events, document cybersecurity issues, and assess the overall impact on organizational operations.
- Performed root cause analysis by mapping identified security problems to underlying vulnerabilities and consolidating related findings into prioritized risk categories.
- Researched and evaluated cybersecurity best practices, developing actionable remediation strategies to address root causes and strengthen the organization's security posture.
- Prioritized security recommendations based on business objectives, operational impact, and risk reduction to align remediation efforts with organizational priorities.
- Authored a formal cybersecurity assessment report detailing

findings, root cause analysis, and prioritized recommendations, incorporating senior analyst feedback before final client delivery.

Threat Modeling for Xibalba Interactive:

https://drive.google.com/drive/folders/1syKQWtQu3yKhe0EMdRF_T0bNcNkZqzmg?usp=drive_link

- Conducted a comprehensive threat modeling assessment by identifying high-risk threat actors, likely attack scenarios, and critical attack surfaces within a simulated enterprise environment.
- Evaluated organizational risk exposure and developed layered defensive recommendations, including honeypot deployment, threat detection strategies, and security mitigations aligned with industry best practices.
- Applied structured threat modeling methodologies to analyze potential attack vectors and prioritize security controls based on risk and business impact.
- Authored a professional threat model report featuring an executive summary, technical findings, and prioritized security recommendations for stakeholder and management review.
- Prepared project documentation for senior cybersecurity analyst review, organizing deliverables in a structured repository while incorporating professional documentation and reporting standards.

Develop an Incident Response Plan:

https://docs.google.com/document/d/1Oubwx0BgD1L35C3yf4YKDwGRpt25UTeMWUygVoEoAhI/edit?usp=sharing

- Reviewed and revised an enterprise Incident Response Plan (IRP), correcting outdated procedures and aligning policies with NIST incident response best practices to improve organizational cyber resilience.
- Validated and updated incident response objectives, team roles, communication procedures, KPIs, and review processes to strengthen incident preparedness and regulatory compliance.
- Evaluated and enhanced incident response playbooks for malware, phishing, and distributed denial-of-service (DDoS) attacks by implementing industry-standard containment, eradication, recovery, and communication procedures.
- Assessed incident response tools, mitigation strategies, and security controls to improve threat detection, incident handling, and continuous improvement across the incident response lifecycle.
- Produced comprehensive security documentation and policy recommendations, ensuring technical accuracy through structured review while supporting stakeholder readiness and organizational security posture.

Network Modernization Presentation:

https://docs.google.com/document/d/1beTuCmkDeGyQumj3QhRA3rGeQWdN-o5yIpDu1Y6GE84/edit?usp=sharing

- Developed a comprehensive Network Modernization Proposal by assessing legacy infrastructure, identifying critical assets, and evaluating cybersecurity risks to improve organizational security posture and acquisition readiness.
- Designed a phased network hardening strategy that established system inventory processes, implemented foundational security controls, and strengthened cyber hygiene through industry best practices.
- Recommended infrastructure modernization initiatives, including secure architecture improvements, technology upgrades, and migration planning to reduce risk and enhance operational resilience.
- Evaluated long-term security operations capabilities by assessing monitoring requirements, recommending appropriate SOC/SNOC strategies, and identifying opportunities to automate incident response through SOAR solutions.
- Authored executive-ready documentation outlining security governance, operational policies, continuous monitoring, and business continuity recommendations to improve day-to-day IT operations and increase stakeholder confidence.

Vulnerability Assessment:

https://drive.google.com/drive/folders/1fAQKmFhFeeL7KBQjxxrJ-IxEI5-Ug1x8?usp=drive_link

- Conducted a comprehensive vulnerability assessment across enterprise hosts, identifying and prioritizing critical, high, medium, and low-risk vulnerabilities based on severity and potential business impact.
- Authored a formal executive-level vulnerability assessment report, summarizing security findings, affected systems, risk exposure, and remediation priorities in clear, stakeholder-friendly language.
- Analyzed vulnerability trends and remediation patterns to identify recurring security weaknesses and recommend risk-based mitigation strategies aligned with cybersecurity best practices.
- Created and incorporated visual security metrics and charts to communicate assessment results, vulnerability distribution, and remediation progress, improving executive decision-making and reporting clarity.
- Produced actionable remediation recommendations by prioritizing critical vulnerabilities, reducing organizational attack surface, and supporting a structured vulnerability management and risk reduction program.

Pentesting report:

https://docs.google.com/document/d/1Z76noJ-LL1iajStRoZVeE-uLDeHNk4Y-aFpNiSfdPXE/edit?usp=drivesdk

- Conducted a web application penetration test against a scoped target environment to validate whether previously identified vulnerabilities were exploitable and assess overall security risk.
- Performed reconnaissance and information gathering using network connectivity testing, target enumeration, and

WordPress application analysis to identify potential attack vectors within the defined engagement scope.
- Executed controlled exploitation of identified vulnerabilities while adhering to Rules of Engagement (RoE), avoiding unauthorized activities such as brute-force attacks, denial-of-service testing, or data modification.
- Documented technical findings in a professional penetration testing report, including executive summaries, testing methodology, proof-of-concept exploitation steps, risk assessments, business impact, and post-exploitation results.
- Developed prioritized remediation recommendations aligned with cybersecurity best practices, enabling stakeholders to mitigate identified vulnerabilities and strengthen the security posture of public-facing web services.

Remediation Report:

https://drive.google.com/drive/folders/1j0HPydbHhJfRRBcV3LRFx5QLaRRQIJHF?usp=drive_link

- Utilized Wireshark to analyze network traffic, identify malicious or anomalous communications, and validate vulnerabilities affecting enterprise network infrastructure.
- Implemented vulnerability remediation through configuration changes, security hardening, and patch validation, ensuring corrective actions were applied to affected network assets.
- Verified remediation effectiveness by comparing pre- and post-remediation PCAP captures, documenting changes in network traffic and confirming the elimination of identified security issues.
- Produced comprehensive technical documentation detailing remediation actions, supporting evidence (PCAPs, configuration modifications, commands executed, and security alerts), and validation of implemented fixes.
- Developed risk-based recommendations for continuous network monitoring, ongoing vulnerability management, and security posture improvements, helping reduce future attack surface and strengthen organizational defenses.

Atomic Red Team Testing and SIEM Deployment

- Executed Atomic Red Team (ART) attack simulations on Windows endpoints using PowerShell to emulate MITRE ATT&CK techniques, including registry modification, process injection, and scheduled task persistence, within a controlled lab environment.
- Monitored and correlated Sysmon telemetry in Wazuh SIEM with local Windows Event Viewer logs, validating attack execution through process creation events, command-line artifacts, timestamps, and MITRE ATT&CK mappings.
- Evaluated the effectiveness of Wazuh detection rules by identifying missed detections, false negatives, and rule coverage gaps, providing insight into SIEM visibility and opportunities for detection engineering improvements.
- Performed log correlation and threat hunting using attack commands, event IDs, and IOC-based pivots to trace simulated adversary activity from endpoint execution through centralized SIEM ingestion and alert generation.

- Executed attack cleanup procedures, adjusted PowerShell execution timeouts for long-running tests, and documented findings to support SIEM tuning, detection validation, and continuous improvement of endpoint monitoring capabilities.

Triage Alerts and IR Report

https://docs.google.com/document/d/1kZQo0qIKhyNWyTW7gps-yTiKwkSx5bsuM9VFB9jj86U/edit?usp=drivesdk

- Investigated network security alerts by analyzing packet captures in Wireshark and correlating events with Splunk logs to identify suspicious activity and determine incident scope.
- Performed alert triage by distinguishing legitimate threats from false positives through network traffic analysis, log correlation, and timeline reconstruction.
- Leveraged Splunk searches to investigate indicators of compromise (IOCs), validate security events, and support evidence-based incident analysis.
- Documented findings in a formal Incident Response Report, detailing the attack timeline, affected systems, root cause, impact assessment, and recommended containment and remediation actions.
- Applied incident response best practices to prioritize alerts, preserve forensic evidence, and communicate technical findings clearly to support effective security operations and continuous process improvement.

Formal Incident Triage Report on a major investigation.

https://docs.google.com/document/d/1D38f6E7cmhv9InQ4iL6Qtt_qEGQ0z8b5QDa6kfWGzKs/edit?usp=drivesdk

- Investigated a high-severity cybersecurity incident using Splunk to triage alerts, correlate logs, and reconstruct the full attack lifecycle from initial access through ransomware execution.
- Identified and documented multiple MITRE ATT&CK techniques, including Brute Force (T1110.001), Active Scanning (T1595.002), Steganography, Data Encrypted for Impact (T1486), and Website Defacement, by analyzing authentication, network, and endpoint telemetry.
- Correlated evidence across Sysmon, Suricata, OSINT, and Splunk to trace attacker infrastructure, validate indicators of compromise (IOCs), identify command-and-control communications, and attribute malicious activity to known threat actor techniques.
- Authored a comprehensive Incident Response Report detailing the attack timeline, root cause, affected assets, forensic evidence, business impact, and prioritized containment, eradication, and recovery recommendations.
- Developed actionable security recommendations, including multi-factor authentication (MFA), stronger password and account lockout policies, enhanced network intrusion detection, endpoint behavioral protection, and secure backup strategies to reduce the risk of future ransomware and credential-based attacks.

Incident Report for a complex attack

https://docs.google.com/document/d/1JKBQZ-sw1ZDfyyWFA059YHSMQaa_1-LdCgijHruHZNY/edit?usp=drivesdk

- **Conducted a comprehensive Splunk-based incident investigation of a complex multi-stage cyberattack, triaging high-severity alerts and reconstructing the complete attack timeline from initial access through command-and-control activity and privilege escalation.**
- **Correlated evidence across AWS CloudTrail, endpoint, authentication, network, and email logs to identify cloud misconfigurations, compromised IAM credentials, phishing activity, malware execution, cryptomining, brute-force attacks, and persistence mechanisms.**
- **Mapped attacker behavior to the MITRE ATT&CK framework, documenting techniques including Valid Accounts (T1078), Brute Force (T1110), Phishing (T1566), Resource Hijacking (T1496), Command and Control, Privilege Escalation, Local Account Creation (T1136.001), and Data Discovery (T1005).**
- **Leveraged OSINT, hash analysis, Base64 decoding, IP reputation research, and log correlation to identify malicious infrastructure, validate indicators of compromise (IOCs), and assess the impact across six compromised endpoints.**
- **Authored a detailed Incident Response Report summarizing forensic findings, attack chronology, affected assets, business impact, and prioritized containment, eradication, and cloud security recommendations, including IAM hardening, S3 access controls, credential rotation, MFA, and enhanced monitoring.**