Gregory W. MacPherson, CISSP, CCNA, ITILv3, SECURITY+

Monroe, WA 98272 | (425) 260-1883 | greg@constellationsecurity.com

# Profile

Greg MacPherson is an experienced technology leader with thirty years of cybersecurity experience. Greg is an intuitive, responsive visionary who designs, manages and implements elegant solutions for large-scale projects. Greg evangelizes improving security of the enterprise by implementing greater visibility into the existing network infrastructure. At AT&T, Greg contributes to planning, provides strategic direction, delivers tactical results and mitigates risk, complexity and threats. Before joining AT&T, Greg worked for Verizon Business evaluating and compromising various cybersecurity products. Greg has been an independent cybersecurity consultant for the public sector and for private sector companies and organizations including AT&T, HP, IBM and Nortel.

# Executive Summary

## LEADERSHIP AND Technical SKILLS

International Business | Incident Response | Process Improvement | Decision Making | Strategic Planning | Budgeting

Recruiting/Hiring | Quality Assurance | Regulatory Compliance | Research & Development | Network Administration

Software Development | CyberSecurity | Security Audits | Software Engineering | Telecommunications | Training

## Selected Highlights

* Championed increased automation and integration using cybersecurity tools and processes.
* Engineered and deployed Microsoft OCS 2007 R2 enterprise-wide.
* Identified and resolved numerous security issues on complex systems and enterprise environments.
* Improved production system performance and reliability.
* Guided and supervised teams of network engineers and cybersecurity experts.
* Directed the architecture and deployment of a secure enterprise wireless network.
* Maintained 100% uptime for critical production system functions.
* Managed equipment specification and purchasing and system administration.
* Managed international telecommunications systems in Brussels, Belgium and Paris, France.
* Reduced costs by proposing, designing and building a standardized pilot program machine.
* Researched, certified, and deployed new and innovative security technologies.
* Spearheaded development of automation of performance metrics for supervisory managers.

## Technical Summary

* **Automation:** Ansible, assembler language, C, CACTI, PERL, Python, ServiceNow, shell scripting, etc.
* **Firewalls:** Checkpoint, Cisco, F5, Fortinet, Juniper, Linksys, Netgear, Palo Alto, PFSense, etc.
* **IDS, Load Balancers, Proxies:** Bluecoat, Cisco, F5, FireEye, Juniper, SourceFire, Symantec, TippingPoint, etc.
* **Network Administration:** BGP, DNS, ICMP, LAN, OSPF, TACACS+, TCP, UDP, WAN, WEP, WPA, 802.x, etc.
* **Security Tools:** Cisco CSM, Juniper JSA, Panorama, Juniper NSM, SNORT, JunoSPACE, SPLUNK, Tenable, Wireshark, etc.
* **Cloud Platforms:** AT&T Integrated Cloud (AIC), AWS, AZURE, Google, OpenStack, etc.
* **VPN:** Cisco AnyConnect, IPSEC, Juniper, Netgear, Nokia, L2TP, PPTP, IPSEC, SSL, TLS, etc.

# Academic and Industry Credentials

## B.S. COmputer Science, Clemson University | CCNA, CISSP, ITILv3, SEcurity+

# Presentations

* *Proactive Security - Book (2024)*
* *Animal Farm Attack - AT&T Data Science Summit (2023)*
* *Cybersecurity Solutions for Pandemic Problems (2021)*
* *Unintended Consequences (SolarWinds) - AT&T (2021)*
* *IPv6 Vulnerabilities - AT&T (2017)*
* *Hiding Evidence of Intrusion in Log Files - AT&T (2017)*
* *Passwords - AT&T (2016)*
* *History of Hacking V2 - AT&T (2015)*
* *Thirty Years of Computer Security US Cybercrime Conference (2014)*
* *I'll Hack You For Christmas - NAISG (2011)*
* *Fun at the Airport - 2600 (2010)*
* *Chicken Wire Fortresses - NAISG (2009)*

Gregory W. MacPherson, CISSP, CCNA, ITILv3

# Experience

## PRINCIPAL MEMBER OF TECHNICAL STAFF, CHIEF SECURITY OFFICE | AT&T | APRIL 2021 - CURRENT

* Advise and provide stewardship for the ongoing governance risk and compliance transformation to ServiceNow.
* Collaborate on architecture, design and development of security solutions and policy in the AT&T CSO.
* Consult and support cybersecurity efforts affecting the Chief Security Organization (CSO) as well as other AT&T business units.
* Develop strategy, processes and document risk and assurance with senior management and technical team members.
* Research and document generative AI (GenAI) security vulnerabilities and lead reviewer for GenAI use cases.
* Support Technical Strategies and Standards (TSS) to support technology transformation and improve efficiencies.

## SENIOR TECHNOLOGY Security | AT&T Mobility | May 2014 – MARCH 2021

* Advise and recommend technology changes to maintain operational security and compliance requirements.
* Automate continuous improvement of new and existing processes within internal security guidelines.
* Continually reassess and analyze global network security threats and operational cybersecurity requirements.
* Coordinate operational security incident response and root cause analysis for global carrier network infrastructure.
* Identify and mitigate security vulnerabilities of firewalls, intrusion detection systems, and network security devices.
* Identify, address, and communicate security vulnerabilities relevant to the deployed security technologies.
* Manage 24/7 surveillance, maintenance, and implementation of physical and virtual production security systems.
* Oversee and coordinate technical security operational projects involving disparate technical teams
* Provide evidence for compliance requirements for PCI, NIST, ISO27001 audits efforts.
* Provide guidance and training in operational cybersecurity risk protection to employees and contractors.
* Public trust position (expires 12/2024)
* Senior Security (IDS/IPS/firewall) SME for Technology Security Organization – Security Lifecycle.
* Serve as a subject matter expert for various firewall and intrusion prevention/detection system security technologies.
* Support globally deployed workforce of multiple technical team leads across a complex organization.

## Principal IT Security Consultant | Constellation Security LLC | January 2010 – December 2018

* Architected and deployed UCS solution across North America.
* Assessed security for Outlook 365 hosted email service.
* Assessed vulnerabilities and performed security incident response for global production network operations.
* Configured security to protect state regulatory agency infrastructure and performed network assessment of infrastructure.
* Created, demonstrated, and promoted automation efforts to support firewall provisioning.
* Deployed intrusion detection system across 14,000-person enterprise to resolve audit findings.
* Discovered and mitigated vulnerabilities in Rapid7 NeXpose vulnerability scanning appliance.
* Managed, configured, upgraded and patched F5 BigIP load balancer/AFM devices worldwide.
* Optimized VPN connectivity for 3,000+ employees and customers. Reconfigured DNS operations across entire enterprise.
* Lead security resource for Office 365 NIST/FISMA compliance effort.
* Resolved networking, performance, load balancing and security issues for 2,000+ firm.

## Senior Network & Information Security Engineer| Verizon Business | december 2007 - december 2009

* Lead engineering and network security team resource for US$6 billion Weyerhaeuser divestiture effort.
* Architected departmental network security R&D research lab facilities in Ashburn, VA facility.
* Created technical articles, requirements documents, statements of work, and vulnerability assessments.
* Identified and documented security vulnerabilities in Cisco, Juniper and Motorola security appliances.
* Identified and mitigated exploitation of multiple vulnerabilities affecting all Cisco ASA/PIX/FWSM firewalls.

Additional work experience available upon request