Gregory Pothier

Highly motivated, proactive, and accomplished NSA Scholar and Senior Security Engineer with 13+ years of hands-on experience building, automating, and maturing the security posture of early stage multi-billion dollar startups, intelligence agencies, and military installations at scale.

✉ gpothier@pm.me
⌂ pothier.io
San Francisco, CA
in gregorypothier

Professional Experience

PRODUCT SECURITY ENGINEER - THREAT DETECTIONS — Mar 2020 - now

Crowdstrike — *Remote*

- Serve as a member of the threat detection and response team leveraging large scale data along with threat intelligence to identify patterns of anomalous behavior, misconfigurations, and indicators of attacks.
- Serve as a member of Crowdstrike's Advanced products team building cloud security products including CSPM, CWPP, and CIEM for AWS, Azure, and GCP.
- Led the cross functional generative AI security detections initiative with the Machine Learning and Data Science Teams including proper ingestion, processing, and normalization of customer security logging and events.

SENIOR SECURITY ENGINEER — Mar 2017 - Aug 2019

Cruise Automation — *San Francisco, CA*

- Successfully architected and developed the security logging and SIEM solution with SOAR tooling integrations.
- Led several security initiatives including incident response, vulnerability management, and threat detection.
- Thrived in a fast paced startup environment, built and led a team of 5 security engineers while securing the internal infrastructure and responding to numerous security incidents.
- Hardened the CI/CD pipelines and Kubernetes while maturing the security of the devops and SDLC processes.

SENIOR SECURITY ENGINEER — Jan 2016 - Nov 2017

Tanium — *San Francisco, CA*

- Led the effort to secure Tanium's infrastructure with its own product and while doing so designed, developed, and deployed multiple software products which became modules for the Tanium product itself.
- Developed the security orchestration and response tooling for automated detection and response actions.
- Led internal security monitoring, threat detection, incident response, patch management, and vulnerability management.

GS-13 SENIOR SECURITY ENGINEER — Oct 2013 - Dec 2015

US National Geospatial-Intelligence Agency — *Springfield, VA*

- Led the "hunting effort" for malicious activity on all NGA networks and systems and briefed senior leadership on the resulting trends of advanced persistent threat activity.

GS-11 SECURITY ENGINEER — Aug 2011 - Oct 2013

US Navy — *Washington, DC*

- Designed and developed an engineering blueprint for the technology architecture and methodology of a Navy Secure Operations Center.
- Honored with multiple performance awards recognizing superior achievement.

ANDROID DEVELOPER — Oct 2010 - Jul 2012

Intellitech LLC — *Washington, DC*

- 100,000+ downloads of paid apps with an average Google Play store rating of 4.6/5.0.

Skills and Certifications

Languages:

- Currently use: Python, Bash, SPL.
- Previously used: Java, C, SQL, Golang, Javascript, React, Node.

Technologies:

- Cloud Providers: AWS, GCP.

- Containerization: Docker, Kubernetes.
- Infrastructure as Code: Terraform.
- Security Tools: Crowdstrike, Carbon Black, OSQuery, GRR, Vault, Tanium.
- CI/CD: Jenkins, Appsec.

Other Skills:

- Threat Modeling, Automation, Incident Handling, Security Engineering, Detection and Response, Vulnerability Management, Penetration Testing, Infrastructure Security, Application Security, Data Loss Prevention, Compliance, PCI, GDPR, Cloud Security Alliance (CSA), ISO 27001.

Certifications:

- 2023 Certified Kubernetes Administrator CKA
- 2022 AWS Certified Solutions Architect Associate (SAA-C03)
- 2016 ELS Professional Penetration Tester
- 2015 Certified Ethical Hacker
- 2014 CISSP
- 2012 CompTIA Security+
- 2013 CompTIA Network+

Education

M. Sc. in Computer Science Information Security 2012

George Mason University *Fairfax, VA*

- Awarded full ride NSA Scholarship for graduate school

B. Sc. in Information Security 2010

George Mason University *Fairfax, VA*

- Awarded numerous SMART grants

Talks, Projects, Publications, and Community

Technical Writings

Tracking Mean Time to Patch Mar 2017

https://www.tanium.com/blog/track-mean-time-patch-4-part-blog-series/

Tracking Critical Compliance Metrics Mar 2017

https://www.tanium.com/blog/track-critical-compliance-metrics-4-part-blog-series/

Tracking Mean Time to Respond Feb 2017

https://www.tanium.com/blog/track-mean-time-respond-4-part-blog-series/

Tracking Critical Vulnerabilities Feb 2017

https://www.tanium.com/blog/track-critical-vulnerabilities-4-part-blog-series/

Conference Talks

Offensive Cyber Hunting: Deploying Deceptive Tools and Tactics 2018

Deception Toolkit leveraging python and Splunk *San Francisco, CA*

Risk Scoring the Enterprise 2017

Automated Risk Scoring Framework for Detection, Orchestration, and Response *San Francisco, CA*

Community Work

Founder and Chief Executive Officer August 2008 - May 2012

Computers For Our Community *Fairfax, VA*