Tesla Careers

Go to search

Security Automation Engineer, Incident Response

Job Category	Engineering & Information Technology
Location	Fremont, California
Req. ID	96082
Job Type	Full-time

APPLY

Tesla participates in the E-Verify Program

What to Expect

- We are looking for a highly motivated engineer specializing in security process automation and incident response to defend Tesla's information, infrastructure, and products. It's fun to work in a company where employees believe in what they're doing! The Detection and Incident Response Team is responsible for detecting and responding to threats against our corporate, manufacturing and production environments. This is a technical role, which is involved in all aspects of the incident response life cycle and what technical steps are needed to automate the process of responding to a security incident. As an Incident Response Engineer, you will be an Incident Handler as part of the Detection and Incident Response team. You will protect Tesla by investigating, containing, remediating, and documenting security incidents. You will also help detection engineers to improve logging coverage, security tools tuning, suggest ideas and contribute to the new signals development process and automation to detect and respond to threats automatically and at scale. Your responsibilities will also include improving/documenting

automatically and at scale. Your responsibilities will also include improving/documenting incident response procedures and playbooks, reporting, and developing and maintaining new automated processes to lower the meantime to remediation.

What You'll Do

- · Participate in incident management calls and coordinate response, triage, recovery, and reporting of incidents. · Monthly and quarterly incident analysis and stats reporting · Ongoing maintenance and improvements/tuning of automated incident response processes. · Work closely with the Detection and Threat Intel engineers to detect, respond to alerts and provide timely response for the security incidents · Participate in incident response activities (including tabletop exercises) to verify existing playbooks and procedures and identify opportunities for improvement · Assessing and analyzing prior incidents for operational improvements, whether automated or manual. · Continuous monitoring, tuning, hardening and improvement of the existing security rules and policies · Keeping existing runbooks up to date and creating new runbooks to improve processes/coverage · Analyze security data and report on threats and incidents across various platforms and environments. · Monitor and analyze emerging threats, vulnerabilities, and exploits. · Provide security monitoring and incident response services supporting the mission to protect Tesla · Security process improvement

What You'll Bring

- · Excellent understanding and experience in multiple security domains such as intrusion detection, incident response, malware analysis, application security, and forensics. · Experience detecting abuse and large-scale attacks in a diverse environment. · Experience in cloud environments (AWS preferred) and Linux containers and orchestration systems (Kubernetes preferred) · Knowledge of web-services such as API and REST · Experience with GIT or other version control systems · Basic understanding of the Security automation (SOAR) principles. As a bonus – ability to implement automated solutions outside of the scope of SOAR. · Experience working with multiple stakeholders such as engineering/operations teams, internal business units, external incident response teams, and law enforcement throughout the incident lifecycle. · Solid experience and the ability to analyze network traffic, endpoint indicators, IOCs. Ability to combine/search/correlate various log sources to identify potential threats, assess the potential damage, and recommend countermeasures · Familiarity with the following detection-related disciplines with deep experience in one or more: o Large scale analysis of log data using tools such as Splunk or ELK. o File system, memory, or live response on Windows, MacOS and/or Linux. o Analysis of network traffic from intrusion detection systems and flow monitoring systems. o Host level detection with tools such as auditd, os-query, SysMon · Real world experience using at least one major SIEM system · Experience with Splunk is a bonus · Security Certifications (i.e. Security+, CISSP, CEH, SANS, etc.) is also a plus

Tesla is an Equal Opportunity / Affirmative Action employer committed to diversity in the workplace. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, age, national origin, disability, protected veteran status, gender identity or any other factor protected by applicable federal, state or local laws.

Tesla is also committed to working with and providing reasonable accommodations to individuals with disabilities. Please let your recruiter know if you need an accommodation at any point during the interview process.

For quick access to screen reading technology compatible with this site click here to download a free compatible screen reader (free step by step tutorial can be found here). Please contact accommodationrequest@tesla.com for additional information or to request accommodations.

Privacy is a top priority for Tesla. We build it into our products and view it as an essential part of our business. To understand more about the data we collect and process as part of your application, please view our Tesla Talent Privacy Notice.