Jordan Reid

Email: hire@jordanreid.me
Website: https://jordanreid.me

EXPERIENCE

Senior Security Detection Engineer October 2023 – Present
Atlassian – Detection & Response

Security Detection Engineer January 2022 – September 2023
Atlassian – Security Intelligence

- Developed high-fidelity detections across a range of log sources and attacker TTPs to detect malicious activity targeting Atlassian and its customers, which improved the detection coverage and security posture of the organisation
    - Includes mapping to the MITRE ATT&CK framework, creating detection logic, and writing detailed documentation and alert response steps
    - Engaged and coordinated with internal and external teams to improve logging coverage, and fix bugs in telemetry tooling
- Led a project to identify, scope, and prioritise gaps in CI/CD detection coverage
    - Researched and documented 30+ systems involved in CI/CD pipelines, both those offered as a customer-facing service by Atlassian, and those used internally by engineering teams across the company
    - Modelled potential threats to the CI/CD platforms, identified opportunities to expand detection coverage, communicated progress with stakeholders, and prioritised attacker techniques to be researched by the team
- Mentored, peer reviewed, and provided feedback to cross-geo team members on detections, tasks, and documentation
- Conducted hypothesis-based threat hunting, and assisted Incident Response investigations across Splunk, Databricks, AWS CloudTrail logs, and other tools
- Identified, maintained, and fixed issues with services in the detection pipeline
    - Improved performance of production detection pipeline by 3x, reducing analyst time spent pushing updates to detections from 2-3 mins to ~40 secs
    - Discovered, managed, and resolved an incident where the alerting pipeline failed to generate alerts in the team's ticketing system
- Ran weekly threat intelligence sessions to identify and research emerging attacker trends and technologies which may impact the company
- Tuned and improved existing detections
    - E.g. fixed a detection that logically could not fire and improved its runtime from 40 mins to 23 secs (a ~100x improvement)

- Continually innovated and improved processes during 20% time, Innovation Weeks, and hackathons, including utilising programming and scripting languages (Python, JavaScript) to create:
  - » a cross-browser extension that provides Splunk info and optimisation tips that was voted 27th/146 projects across APAC during a hackathon
  - » a Splunk add-on with custom Splunk search commands to enrich queries with data from internal APIs
  - » a userscript to add visual multiline diffs to Jira ticket history
  - » a script to automate bulk detection updates
  - » Splunk macros that simplified, and standardised common parts of queries
- Team placed 1st out of 238 participants in Splunk's APAC BOTS 2022
  - » Individually scored 52.9% of the team's points

Senior Security Analyst November 2020 – December 2021
DXC Technology – Cyber Security Incident Management

- Senior point of contact for the SOC team and customers
- Managed and responded to security incidents
- Consolidated metrics which led to a reduction of alert noise by 50%
- Automated report creation, reducing preparation from 10+ hrs/month to 30 mins

Security Analyst September 2018 – October 2020
DXC Technology – Security Operations Centre

EDUCATION AND TRAINING

Linux Enterprise Incident Response 2022
Mandiant

Bachelor of Science in Computer Science (Networks) 2018
University of New South Wales

- Ernst & Young Prize for the Best Performance in Securing Wireless Networks

Bachelor of Science in Psychology 2018
University of New South Wales

REFERENCES (CONTACT DETAILS AVAILABLE UPON REQUEST)

- Emma Ferguson (formerly Security Intelligence Team Lead, Atlassian)
- Ashley Blackmore (Principal Security Engineer, Atlassian)