64 Whin Knoll Avenue
Keighley
West Yorkshire
07476966379
dyl.hearn@gmail.com
AchillesDH

Dylan Hearn

Professional Profile

Cyber Security Engineer with 4+ years of experience in automation, incident response, malware analysis, programming, and customer engagements. Proven ability to lead SIEM & SOAR onboarding, migrations and automations, develop custom tooling, with a mix of cloud and on-premise solutioning. Delivered vulnerability management and web application security reports for customers with a mixture of automated and manual testing.

Experience

Sep. 2022 - Present — **Cyber Security Engineer**, *SEP2*

- Collaborate with clients to automate, orchestrate, and bolster their security operations, tailoring solutions to ensure an optimal balance between automation, reliability, and ease of use, aligning with their bespoke workflow demands.
- Carry out professional services work for customers, including a major banking provider, meeting the provided requirements, and working with key stakeholders e.g. CISO, SOC manager, ensuring the solution met all their needs.
- Serve as escalation point, providing guidance to analysts, and liaising with customers to mitigate risk where possible.
- Investigate and resolve escalated security cases, including DFIR, reverse engineering, and malware analysis, to identify root causes and recommend or enact mitigation and prevention strategies where necessary, adhering to PICERL.
- Created a reliable and efficient Chronicle SOAR connector, integration, job, playbook, and remote agent monitoring solution, using undocumented endpoints asynchronously, ensuring high fidelity actionable alerting with redundancy.
- Designed a git based CI/CD pipeline for rule creation and modification, allowing for automated testing, validation, and submission, while ensuring cross tenant separation.
- Improved customer onboarding efficiency via strategic automation combined with a structured approach, documenting the process, deviations, impacts, trade-offs, and possible pitfalls.
- Create and review changes to rules, playbooks, custom actions, parsers, and other infrastructure. Source ideas from analysis team lead and the wider analysis teams, ensuring a collaborative and inclusive approach.
- Designed and documented a process for building custom SOAR integrations, and connectors, ensuring a consistent methodology, including following Python best practices and extensive testing.
- Developed Chronicle SOAR integrations/connectors for unsupported platforms, such as Area 1, Code42, MS Graph, PagerDuty, and IncidentIO, documenting the process to allow reproducibility and prevent knowledge silos.
- Designed a YARA-L 2.0 rules repository, allowing for a single "base" rule to be adapted to each customer's unique environment, alongside advanced sorting and tagging, ensuring rapid onboarding of relevant rules for a customer.
- Design custom health monitoring rules using Google Cloud Monitoring to ensure strong visibility on potential downtime, and log ingestion issues.
- Migrate existing customer rules from their previous languages (e.g. LPL, SPL, KQL) to YARA-L for use in the Chronicle SIEM while ensuring parity.

Sep. 2020 - Sep. 2022 — **Cyber Security Analyst**, *SEP2*

- Produce monthly Vulnerability Management and Web Application Scanning reports for customers using Qualys and Greenbone.
- Conducted manual web application testing to determine true-positive vulnerabilities that have been found by external scanners.
- Involved in the deployment of Chronicle SIEM and SOAR, enhancing real-time threat detection and incident response capabilities.
- Maintained an extensive repository of YARA-L 2.0 rules, ensuring a strong baseline of detection's and fortifying our many customers' postures and ensuring rules are as vendor agnostic and UDM reliant as possible.
- Designed and implemented Chronicle SOAR playbooks, focusing on automation and efficiency in analyst workflows, including intelligent enrichment, automated UDM searches, and tailored alert descriptions.
- Proactively investigated and swiftly responded to high-priority alerts and complex security incidents, ensuring minimal impact on organisational assets.
- Contributed to the development of our SOC team through in-depth training, elevating their technical proficiency.

Technical & Personal Skills

- Python
- HTML/CSS/JS
- React
- Bash
- VBA
- LaTex
- SQL (SQLite, PostgreSQL)
- NoSQL (MongoDB, Firestore)
- Kubernetes (GKE, EKS)
- Terraform
- Regex
- Selenium (Python)
- Logstash (Chronicle CBN)
- YARA-L 2.0 (Chronicle SIEM)
- LQL (Logscale)
- SPL (Splunk)
- KQL (Sentinel)
- Chronicle SOAR (FKA Siemplify)
- Splunk SOAR (FKA Phantom)
- Looker (Chronicle Dashboards)
- Autopsy
- FTK Imager
- Darktrace
- Metasploit
- Sliver
- Qualys
- Greenbone
- Burp Suite
- GCP
- Azure

Certifications & Training

2021 - 2023 **CySA+, Security+, Network+**, *CompTIA*

2023 **Dantes Lab**, *HackTheBox*

2020 **eJPT**, *INE Security (FKA eLearnSecurity)*

Education

2020 - 2022 **Level 4 Apprenticeship**, Cyber Security Technologist

2016 - 2018 **Level 3 BTEC**, IT

2016 - 2018 **A Levels**, Mathematics, Computer Science

2011 - 2016 **GCSEs**, 7 GCSE's grade C and above

References

Avaliable on request.