Ryan Richardson

ryan@ryan-richardson.co.uk • https://ryan-richardson.co.uk

Personal statement

With over 3 years experience as a SOC analyst in a corporate environment, coupled with multiple years previous to that managing servers as a hobby, I have a wide breadth of knowledge in dealing with Security Incidents as well as the engineering side of these tools. As I also stepped into the interim Head of SOC role, as well as capability build, I've had the opportunity to see working in the SOC from a variety of perspectives.

Key Skills

- Identifying and responding to Security Incidents from various sources, including within a consultancy capability.
- Defining and reviewing processes to ensure alerting can be responded to effectively
- Security tooling deployment, configuration, maintenance and operation.
- Troubleshooting and finding mitigations for issues.
- Working under pressure in time-sensitive scenarios.
- Interfacing with management and senior leadership to showcase capabilities, make them aware of gaps and provide updates on security issues.

Employment History

SOC Analyst at Maersk Line

(June 2017 – Present)

Reporting into the Head of SOC, responsible for providing increase in capability, security incident response, tooling maintenance, creating documentation and the procurement of new tooling across the company's global presence.

Key Achievements:

- Resolving multiple security incidents, some of which had the potential to, or did cause, business impact of various degrees.
- Developing and then running an APT based simulation for the team that went from SOC up to crisis management.
- Becoming a key contact point for senior members of the business in relation to security incidents or questions.
- Demonstrating security capability to the C-level members to show the uplift we've had since the incident.
- Reducing the demand on other members of the team by creating automation to take care of more menial tasks.

Key Responsibilities:

- Investigating, containing, responding to and remediating security incidents.
- Defining processes for the usage of tools and response to alerts.
- Training up new members of staff so they are able to respond effectively.
- Acting as an escalation point, when required, for members of the team including out of hours on-call.

- Creating and running technical incident simulations for the team to baseline capabilities and identify areas for improvement.
- Providing input into projects and procurement attempts from an operational security perspective.

Technical Knowledge

- AV tooling - McAfee, Trend Micro, Microsoft Defender, CrowdStrike
- EDR tooling - CrowdStrike
- Network detection - Trend Micro, DarkTrace
- Ticketing - ServiceNow
- SIEM - Splunk, Sentinel
- Vulnerability Management - Qualys
- Automation - Azure logic apps
- Azure, O365, Linux, Windows

Education

Prospect School

(September 2009 – June 2011)

A-Levels:

- BTEC ICT Practitioner Level 3 national Award
- History
- Government and Politics

(September 2004 – June 2009)

- 5 GCSEs, grade B-C, including Maths and English.
- 4 VCEs, at pass grade, including the European Computer Driving License at level 1 & 2.
- 1 BTEC, at pass grade overall, for an ICT First Diploma at level 2.
    - Broken down to a pass in:
    - Using ICT to present information, website development, installing hardware components and ICT graphics.
    - And a Merit in introduction to computer systems, mobile communications technology and security of ICT systems

Hobbies & Interests

I'm an avid gamer, being previously involved in an international gaming community, which has one of the last, populated, battlefield Vietnam servers and the most popular Minecraft city roleplay server, where I managed the dedicated servers and was the main point of contact regarding problems. I kept the servers running and dealt with bug reports for the website or servers. As part of this role I was involved in talks regarding re-distribution efforts for a game (Battlefield Vietnam) with EA, after contacting their CEO to see what could be done. I've also had to deal with, and resolve or mitigate the effect of attacks on the servers, ranging from a simple Denial of Service attack to Distributed Denial of Service attacks as well as hex editing game files, following advice after reaching out to third parties, to prevent the use of exploits in the game. This is what gave me my first insight into security.

In addition, I've come to love travelling internationally and the amazing experiences that it brings. At least until a global pandemic hit...