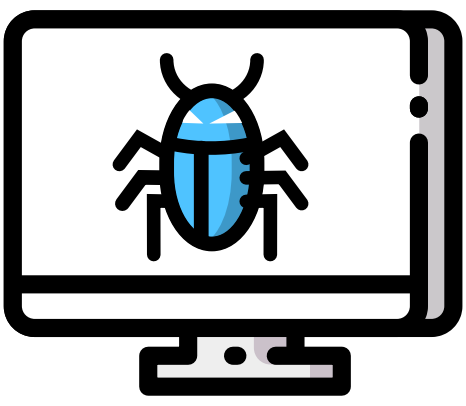
SentinelOne™

WHAT JOBS ARE THERE IN CYBERSECURITY?

THE CYBERSECURITY SKILLS SHORTAGE

The cybersecurity skills shortage is a pressing concern for businesses, with the current shortfall estimated to be around 2 million unfilled positions, a number that is expected to rise to around 3.5 million by 2021. If there's an upside to this shortage, it is that for those interested in a career in cybersecurity, there are many opportunities to enter this vast and interesting field.

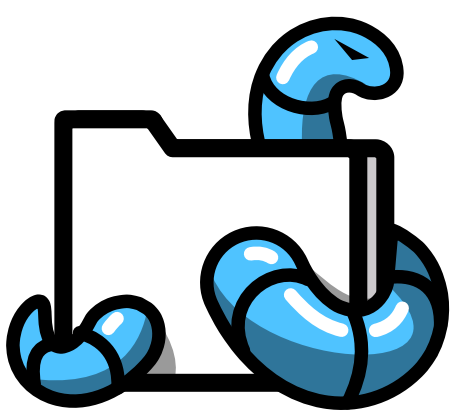


SECURITY ANALYST

Typically works in a Security Operations Centre or IT team focused on security. An analyst's primary job is incident detection and response. Analysts will be required to triage, investigate, contain and remediate cyber security incidents. They will need to use and operate EDR tools. Their duties will also likely include some threat hunting and incident reporting.

PENETRATION TESTER

May be an independent contractor or in-house staff, the "pen testers" job is to simulate real attacks to find weaknesses in an organization's security. Pen testers go further than just looking for vulnerabilities, though, as their job is not just to show that there is a chink in the armor, but to actively prove that it can be exploited.

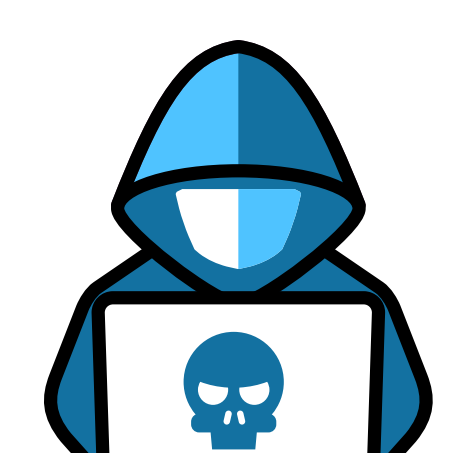


DIGITAL FORENSICS INVESTIGATOR

The work of those involved in DF/IR (digital forensics/incident response) takes place after a digital crime or breach has been found to have taken place. The cyber crime investigator will typically work with law enforcement officers to identify direct evidence of a crime, collect any evidence that may be used in attribution, and to ascertain as much information as possible about the attackers' actions while on the device through examining digital artifacts.

MALWARE RESEARCHER

The role of the malware researcher or analyst is to take code written by threat actors and understand what it does, how it does it, and how the organization's security team can detect it. Crucial to the work of a malware researcher is the ability to reverse engineer malware, which involves understanding the internal functions of a program without having access to its source code.



SentinelOne delivers autonomous endpoint protection through a single agent that successfully prevents, detects and responds to attacks across all major vectors. Designed for extreme ease of use, the S1 platform saves customers time by applying AI to automatically eliminate threats in real time for both on premise and cloud environments and is the only solution to provide full visibility across networks directly from the endpoint.

DISCOVER MORE AT WWW.SENTINELONE.COM

SentinelOne™