PLURALSIGHT

4 ESSENTIAL SKILLS FOR A GOVERNMENT SECURITY ANALYST

Upskill your personnel

BY RICHARD HARPUR

In the government, today's rapid growth of technology is closely followed by the booming threat of cybercrime, driving demand for more cybersecurity professionals. Without multi-disciplined cybersecurity personnel, defending technology assets isn't just difficult––it may be impossible.

One fundamental role your department needs is security analysts. And the good news is that federal workers are incredibly interested in reskilling for this role. According to Nextgov.com, more than 1,500 applications were received for the new Federal Cyber Reskilling Academy in November of 2018.

Progressing from a Level 1 to a Level 3 role requires mastering four fundamental skills

WHAT TO EXPECT FROM A SECURITY ANALYST ROLE

Security analysts work hands-on to understand the activity occurring within their department and to defend it from attack. This may look like investigating security alerts and suspicious activity, establishing and managing threat protection systems or responding to incidents.

Within a Security Operations Center (SOC), security analysts typically work at one of three levels depending on experience. Level 1 is responsible for the majority of triage work. They investigate alerts or suspicious activity to determine priority and urgency. Level 2 analysts should be able to attribute suspicious activity to specific threats. Highly experienced Level 3 analysts undertake detailed analysis and forensic investigation on cyberthreats.

Progressing from a Level 1 to a Level 3 role requires you to master four fundamental skills.

Four essential skills for a Security Analyst

11582-18

1. NETWORKING

To maximize damage, malware and other cybersecurity threats are heavily dependent on computer networks. It's rare to have an attack on a system that's not networked. Even the Stuxnet attack[1], which was launched on highly- protected and segregated systems, was made possible because the systems were networked to an extent. For this reason, it's essential that you're skilled and comfortable with the fundamentals of networking. This includes understanding the OSI network model and network protocols such as TCP/IP.

Frequently, a security analyst will be given key basic information from network device logs. This will most likely include source and destination IP addresses, protocols used and other common networking information. You need to know what each piece of information means and how it might impact your analysis.

2. SECURITY

Once you've developed networking fundamentals, you need to understand security fundamentals. A solid understanding of various cyber threats equips you to know what patterns and behaviors to look for in your analysis.

Various patterns exist for launching a cyber attack. Different malware variants may reuse some of these patterns. Patterns such as command and control are common with Ransomware attacks, for instance. As you trawl through log records, you should be able to quickly identify suspicious or dangerous activity, having mastered the security fundamentals.

The importance of this skill was highlighted with the global outbreak of WannaCry. This ransomware incident originated from eastern Europe and spread rapidly across the globe, hitting the United Kingdom particularly hard. Early on, it was reported the malware was searching for a specific domain name. If the malware could access that domain name then it stopped working, thereby containing the spread of infection. It was effectively an electronic kill switch.

In instances like this, a security analyst well versed in security fundamentals would be able to easily identify the computer IP addresses that were trying to contact the so-called kill switch and deduce that these computers were infected with WannaCry. From there the analyst could arrange for infected computers to be removed from the network and cleaned.

11582-18

3. INCIDENT RESPONSE AND HANDLING

Not all security analysts are involved in incident response, but most are to some degree. The ability to work within a formal incident detection and response process makes the security analyst role that much more valuable to a department.

There are best practices in defending a department's digital assets from attack. Frequently, you're working in a crime scene, so you need to understand the big picture when it comes to incident response. If you delete or modify data, which was going to be relied upon as digital evidence, it might eliminate the option to prosecute the attackers.

4. COMMUNICATING AND DOCUMENTING INCIDENTS

Largely considered a soft skill than the technical skills above, competency in communicating is essential during security incidents. Very often, you'll work as part of a larger team of personnel. Incidents will be escalated and passed around, so good communication helps.

Consider identifying a new zero-day vulnerability. You may need to escalate this to Level 3 SOC members, to vendors or to users of the system. Furthermore, any records of activity or actions taken must be properly documented, as they may be used in a legal proceeding.

SKILLS FOR A SAFER TOMORROW

Of course, there are many additional skills you will develop over time, such as network packet analysis using tools like Wireshark. Many open-source and community-based tools are used extensively by security analysts. As your experience grows, so, too, will your dependency on tooling.

Trends certainly dictate that we will need more and more security analysts over the coming years to accommodate the rise in cybercrime. Whether you're looking at your own service and identifying how to get started as a security analyst, or you're leading personnel that needs to add security analyst skills, keep your focus on these four skills to build your essential skillset.

11582-18