DevSecOps and Detection Engineering: Integrating Social Science Principles into Cybersecurity Practices

Jaden Walker

CYSE201S

Diwakar Yalpi

4/13/2025

Cybersecurity isn't just about technology, it's about people. In today's ever changing technology world, DevSecOps and Detection Engineering professionals are turning to social science ideas. Some examples are studying behavior, practicing solid communication, making ethical decisions, and embracing inclusivity to level up their work. By weaving these people-focused skills into their day-to-day tasks, teams don't just get better at the technical side of things; they also make sure their practices are fair, responsible, and supportive of everyone, including the most marginalized groups.

A good portion of the people-centered approach comes down to recognizing how human behavior influences security, especially for Detection Engineers. They use behavioral analytics to spot odd or dangerous activities in digital systems. For example, AWS shows how tracking a "normal" baseline of user behaviors helps engineers quickly spot weird deviations. This user-focused angle makes threat detection both swift and precise, helping keep digital spaces safe. You can also do the same things "manually", with tools like Splunk, by knowing what normal network traffic looks like via dashboards and spotting anomalies.

In the relatively new field of DevSecOps, communication and collaboration are just as important. By building security into each step of software development, it's important that developers, security pros, and operations teams all stay on the same page when it comes to pushing a product to production. According to Splunk, good teamwork helps uncover and address issues early on by having thought provoking conversations and talking through best case/worst case scenarios. A hidden benefit of operating in a steady back-and-forth way is that it builds trust within the team and fosters a more unified, effective security culture.

Ethics also play a huge part in any field of technology, especially when it comes to handling sensitive data or leveraging AI tools. DevSecOps teams have to protect privacy, fairness, and transparency in everything they do due to the overall premise of DevSecOps being a “One stop shot”. IBM warns about biases and discrimination slipping into AI-driven solutions, reminding us how crucial it is to stay vigilant about any hidden harm technology might cause. By staying transparent and looking out for ethical pitfalls, cybersecurity pros help make sure these powerful tools truly serve the public good.

This commitment to ethics is particularly vital for the betterment of marginalized communities. Designing inclusive security measures means ensuring that stricter authentication or security controls don’t accidentally lock out people with disabilities or those who live in less well-served areas. AWS stresses how being aware of those diverse needs is key to building security solutions that everyone can use.

Detection Engineers face a similar challenge around AI fairness. If analytics tools are trained on biased data, certain groups can end up singled out or unfairly targeted. IBM advocates building fairness into AI from the start, which is crucial for keeping these biases from impacting real people. When done right, this proactive approach safeguards those who might otherwise be most at risk. Detection Engineers also face the constant challenge of deciphering which is a false positive, and what is the real alert. Knowing that context will allow you to gain insight as to why some Detection Engineers were so willing to implement AI.

There is a distinct connection between cybersecurity and society once you understand the duality of public perception. Protecting critical infrastructure in healthcare, finance, and government, cybersecurity builds public trust and confidence in technology. At the same time, people’s

expectations around privacy, ethics, and transparency are constantly shaping how cybersecurity evolves. As threats keep changing, so do the demands for trustworthy, responsible security methods—pushing professionals to adapt and stay in sync with what the public needs.

Ultimately, weaving social science principles into DevSecOps and Detection Engineering makes cybersecurity stronger and more human-focused. By understanding human behavior, communicating well, staying ethically grounded, and being inclusive, cybersecurity teams not only sharpen their tech skills but also help build a safer, more equitable digital future for everyone.

References:

AWS Cloud Adoption Framework: Security perspective. (n.d.-a). https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-caf-security-perspective/aws-caf-security-perspective.pdf

Securing generative AI: What matters now. IBM. (n.d.). https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/securing-generative-ai

What is DevSecOps?. Splunk. (n.d.).

https://www.splunk.com/en_us/blog/learn/devsecops-concepts-principles.html