Security teams are under immense scrutiny today due the increased frequency and sophistication of cyberattacks. Keeping up with the adversary is impossible without expanding the skills and experience of cyber defenders in new directions. So, what does this Dream Team look like? Get these folks on board and know that with these new skills and roles as a part of the CISO’s security team, the whole will truly be greater than the sum of its parts.
Folks in:
Vulnerability management
Threat intelligence
Security operations

Also includes network defense teams, security architecture and blue teams.

They continually monitor and endeavor to harden security around and within the company's networks and data systems.
Red teams
Penetration testers
Ethical hackers

They take an offensive approach to cybersecurity by emulating the behavior of an adversary.

Adept at all forms of digital attack, social engineering etc. to break into systems and continually test the limits of your cybersecurity posture.
The policy expert, the person who says “no” to the employees (or admins) who have risky behavior like phishing or password reuse.

They are responsible for ensuring that the organization is following all compliance best practices.
The software developer or security analyst with secure coding skills.

Helps enable API based integrations of various security products.
The CFO. Cybersecurity is a critical financial risk to the organization.

Cost of cybersecurity is not only related to purchasing tools and hiring resources to avert cyberattacks, but also the potential cost of a breach.
The AI-powered platform that monitors all assets across a broad range of attack vectors in real-time.

It learns the context of your business, continuously analyzes your complete attack surface and predicts where you are likely to be breached.

Utilizes little or no human effort and prescribes the necessary tactical and strategic mitigations to minimize risk and improve cybersecurity posture.