SESSION TITLE	Expanding your Blue Team by Creating Security Culture
SESSION QUICK ABSTRACT	By driving vulnerability reporting through positive incentives and behavioral science, one can enable a "safe to fail" culture with improved results for incident detection and anti-phishing.
SESSION ABSTRACT	In 2012, Salesforce launched a program aimed at increasing the difficulty of a successful phishing attack on their employees. By driving vulnerability reporting through positive incentives and behavioral science, this talk will show how to account for human mistakes to enable a culture where it is "safe to fail" with improved results for incident detection and anti-phishing.
SESSION DETAIL	Often, attackers only need one employee to fall for an attack before gaining a foothold in an organization. The defenders on the other hand have to continuously catch all attacks to keep an organization secure. In 2012, Masha Sedova began a new approach to Salesforce's security awareness program aimed at increasing the difficulty of a successful attack on their employees. The goal was not only educate the company's employees about security, but also to make them invested in their part of securing the company by reporting suspicious activity. After a multi-step approach, the company continues to see increasingly promising results on detecting simulated and real phishing emails and defending against red team exercises. In this talk, Masha will talk about the steps she's taken to increase the reporting of suspicious activity by her employees and the measurable impact it has had in helping keep Salesforce's employees and customers secure. Specifically, this talk will discuss how an organization's relationship to failure affects their ability to respond to an attack and reduce the dwell time of an attacker on their network. The talk will look at how organizations can account for human mistakes and enable a culture where it is "safe to fail" Masha will discuss how using positive incentives and recognition at scale to reward for the correct behavior can create such a culture. The talk will then show results of a culture where reporting of known and suspected vulnerabilities is encouraged and the positive impact on incident detection, improved anti-phishing results, and increased difficulty for red team exercises.