ebay

CUSTOMER PROFILE

Customer
eBay Inc.

Industry
ecommerce

Founded
1995

Location
Global (San Jose, CA)

Tools
Logging platform, SIEM, case management

Decreased detection deployment time by

30%

In regular scenarios

Gained a

20%

increase in security detection coverage of MITRE framework attacks for Windows in the first year of usage

Goals

- Protect the enterprise while enabling widespread innovation toward business goals
- Lessen alert fatigue among security and incident response teams
- Decrease the operational costs of deploying detections

Challenges

- Time to respond and deploy detections to critical incidents was too slow
- Inundating teams with too many false positive alerts
- Inability to keep up with the threat landscape

Highlights

- Decreased detection deployment time by 30% in regular scenarios
- Reduced detection deployment time from 1.5 weeks to 48 hours in emergency scenarios
- Gained a 20% increase in security detection coverage of MITRE framework attacks for Windows in the first year of usage

Background

eBay is a leading ecommerce company that connects millions of buyers and sellers worldwide to create economic opportunities for all. To make these connections, eBay embraces innovation and cutting-edge technology to architect highly scalable systems. Moreover, to enable widespread innovation and drive the business forward, eBay leadership prioritizes security to protect its global consumers and 10K+ employees.

Challenges

Like many organizations, eBay faces common challenges such as delivering fast incident response, alleviating alert fatigue, and scaling resources. Since joining eBay in 2014, Kiran Shirali has had a wide breadth of experience on the security team, including application security, red team, and blue team efforts. In his latest role as Senior Manager of Security Engineering, his primary challenge is implementing proper security detections that catch suspicious activity but don't flood the incident response team with too many benign or false positives. "If an alert is firing too aggressively, there is an operational cost," says Kiran, "We have to reduce alert fatigue for our talented engineers in both the security and infrastructure teams. Their time is valuable and the fatigue demoralizes." Kiran is also concerned about the ever-changing security landscape making it difficult to keep up with the latest threats as eBay expands and grows the business: "As a detection manager, I need to be able to quickly respond and put the appropriate detections in place."

Enter Anvilogic

With the Anvilogic Modern SOC platform, Kiran and his team were able to leverage out-of-the-box detections and research to fine-tune and quickly release detections. Before Anvilogic, it would take the team between four to six weeks to research, test, and tune a detection to ensure a 95% true-positive rate before releasing and deploying it into production. With Anvilogic, eBay shortened that time by up to 30%. In the case of emergency scenarios like a zero-day vulnerability, what would have taken eBay up to a week and a half to deploy a new detection now takes them no more than 48 hours. By democratizing detection engineering efforts and utilizing a no-code threat scenario builder, the team has saved significant time while allowing eBay's security threat hunting team to increase the quality of security detections: "The scenario builder was easy and intuitive. When you have to write detections in a query language, it requires some skill to put your thoughts into that specific code. But with the drag-and-drop interface, it allows the team to experiment with scenarios. It really flattened the learning curve and allowed people to start using Anvilogic right away." Looking forward, Kiran sees Anvilogic as a strategic partner as they continue to push and innovate while still protecting eBay's customers and the overall business, "I get a lot of unrealistic promises [from other vendors], Anvilogic has been a good partner in terms of what problems my team is facing and how to solve them."

> *The greatest strength of Anvilogic is it has a lot of existing research that can easily be taken and deployed in the context of your company.*
>
> – **Kiran Shirali**
>
> *Senior Manager of Security Engineering, eBay*