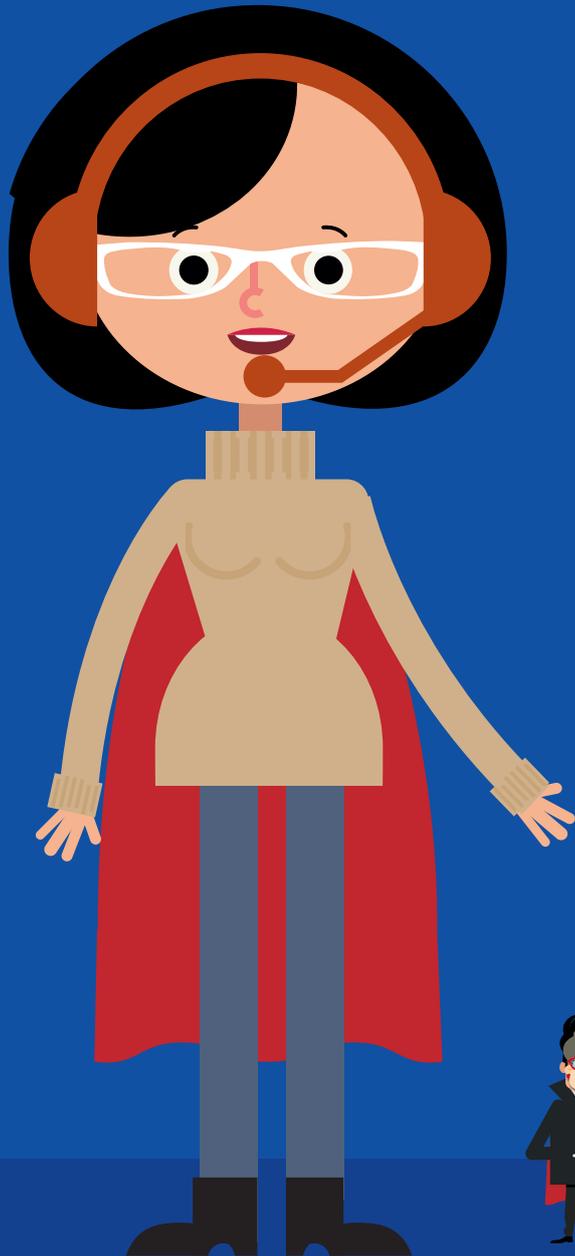

Susan

Our Supply Chain Manager



Meet Susan, The Supply Chain Manager

Susan will supply you with real-time and ongoing indications of any compromises that threaten your supply chain and of any new threats targeting your vendors, partners, or affiliates. Susan makes sure that your supply chain is (at least) as Cyber Ready as you are.

Susan focuses on the potential risks associated with your supply chain; including your external suppliers, vendors and service providers. Susan evaluates the current cybersecurity capabilities of your existing or future vendors.



▲ **The Technology Behind Susan**

Supply chains may be overwhelmingly large and continuously monitoring them can be very complex, which is why Susan utilizes technology that automates 90% of the process.

Susan uses our Argos platform to automate a major part of her operations. Using Argos and her CyberOPS team, Susan monitors the dark web, deep web and open web for any indications of compromise that affect your supply chain. Once she detects an indication of compromise, she'll investigate it with her team, assign a risk score to it, and let you know about it so that you could mitigate the threat and convey the message to your vendor.

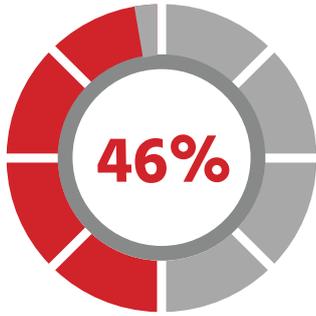
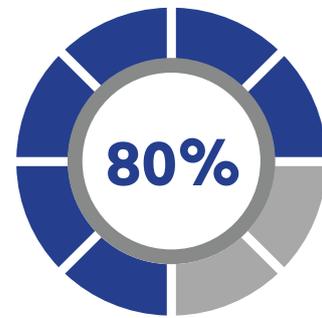
Additionally, Susan can automate random (passive) attack scenarios on your supply chain and provide you with an indication of the supply chains' awareness.

▲ **Why Monitoring your Supply Chain is so Important**

You're only as strong as your weakest link. This is exactly the case when it comes to your supply chain. While your organization may be top-notch in its cyber readiness, your supply chain can ultimately take you down. In order to make sure you're resilient to cyber threats, your supply chain must be as resilient as you are.

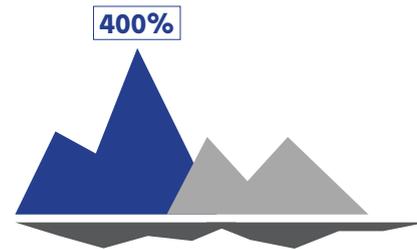
Without Susan, the vulnerabilities of third parties within your ecosystem can easily be exploited by your adversaries who will access your own organization.

* SANS Infosec estimates that **80% of breaches originate in the supply chain.**



* In the SANS risk barometer, **46% of global firms** said business and supply chain was their biggest risk, with the average insurance claim for this type of incident amounting to **896,000 GBP.**

* Since 2012, the Allianz Risk Barometer has assessed that supply chain breaches have **increased by 400%.**



Between **2013** and **2015**; Target, Home Depot, and the U.S. Office of Personnel Management all suffered heavy losses due to data breaches caused by supply chain vendors.

Between these three breaches, the complete amount of stolen credentials involved:

110 Million

of Target customers' data and 40 million of their respective payment cards (SANS Institute).

53 Million

email addresses of Home Depot customers, as well as 56 million of their respective payment cards (Computer World)

22 Million

records belonging to U.S Office of Personnel Employees; Federal and Military Personnel, as well as contractors (SANS Institute).

Susan makes sure that this won't happen to you or to your customers/employees. If any of your suppliers or supply chain vendors are threatened by security, you'll still stay secured, no matter what.