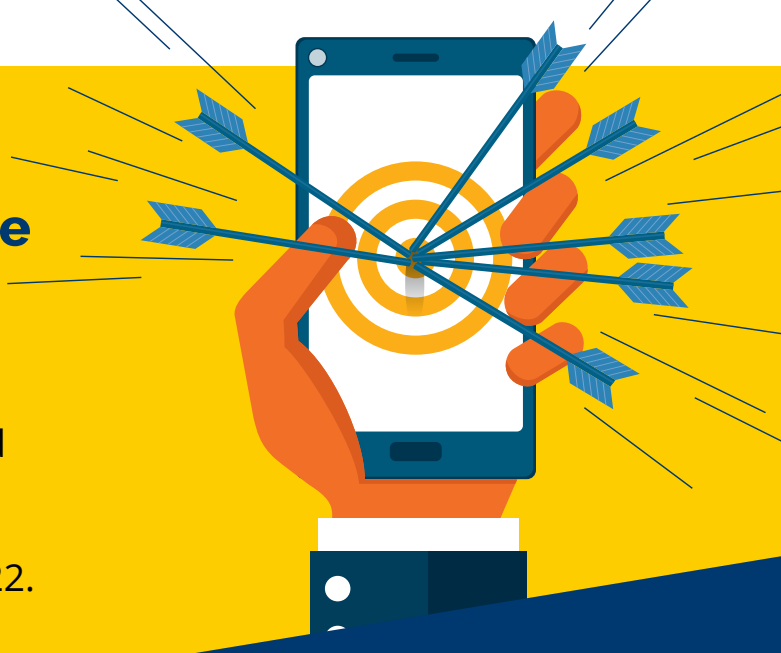
FLARE

Cybersecurity Predictions for 2022



Prediction #1
Cyber Criminals Will Continue To Diversify Their Target

2021 has seen an increase of successful attacks against critical infrastructures: food industries, water treatment, utility companies, gas infrastructure, etc. We expect that this growth will continue in 2022.

Prediction #2
Ransomware Will Continue in 2022 But Shift in a New Direction

- We think that disruption of normal operations will be a bigger threat than disclosing data, especially when it comes to the critical infrastructures
- We will continue to see a shift in ransomware groups' approach, methods, and how they are using vulnerabilities. Ransomware groups may also use new strategies to monetize their attacks
- Insurance companies may no longer pay for ransomware attacks

Prediction #3
2022: The Year of Resilience

We predict that 2022 will be the year of cyber resilience for organizations. Successful organizations will respond and remediate attacks with more resilience, especially as the number of attacks rise.

Prediction #4
A Shift Toward a Zero-Trust Model

Companies are starting to give the right amount of data access to their employees to minimize the potential of human error and its damage. We must ensure that employees have only the information they require to do their tasks effectively.

Prediction #5
2022: The Year of Privacy

At Flare, we have predictions for the concept of privacy in 2022:

- In 2022, consumers will start to increasingly understand the concerns around privacy and will start looking for products that have privacy as a feature
- Organizations don't necessarily know where to start, but they know they want to have more control of their data and more privacy enforced at an organization level
- We think that compliance is going to be the one that pushes privacy forward the most

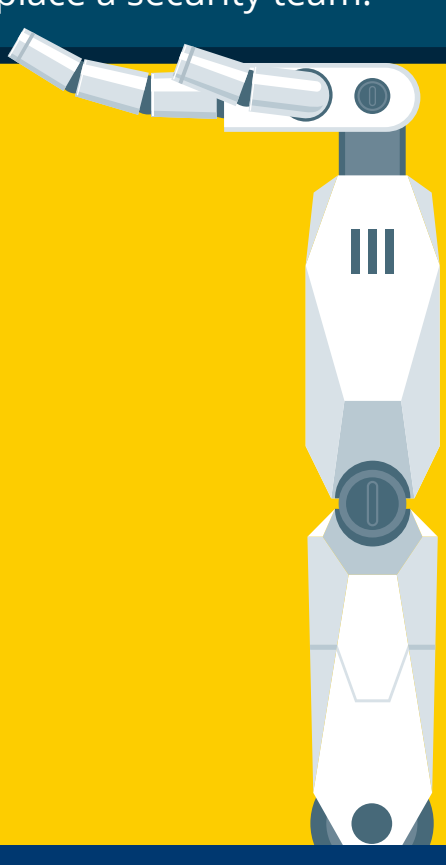
Prediction #6
Dependency Management Software Is Going to Improve

Everything is now moving to containerized applications. The consequence is that, now, patching bugs of this nature is much harder than it was a couple of years ago because it's running in twelve different containers on the same machine. It's running on applications where you don't even necessarily control the build system. Just knowing what apps you're running that are affected is also challenging because **you need to have good dependency management tooling to know that it's running inside that specific container on that specific machine**.

This is where dependency management becomes really important. Only knowing that you have the database running and its specific version is no longer enough.

Prediction #7
Real AI Will Be More and More Used in Cybersecurity

Definition of AI (Artificial Intelligence) in Cybersecurity: It's a tool in order to make decisions. AI does not replace a security team.



According to Forbes, with the major shortage of skilled cybersecurity workers and rapidly growing internet attack surface, the need to automate and use AI will become a market driver for years to come.

Some use cases where we can use AI in cyber:

- Detect patterns in complex data
- Monitor some networks
- Restrain access if malicious actors have suspicious behavior
- Detect malicious transactions for credit card companies
- Cluster and classify the information

Learn more about our solution

Request a Demo

FLARE

https://flare.systems