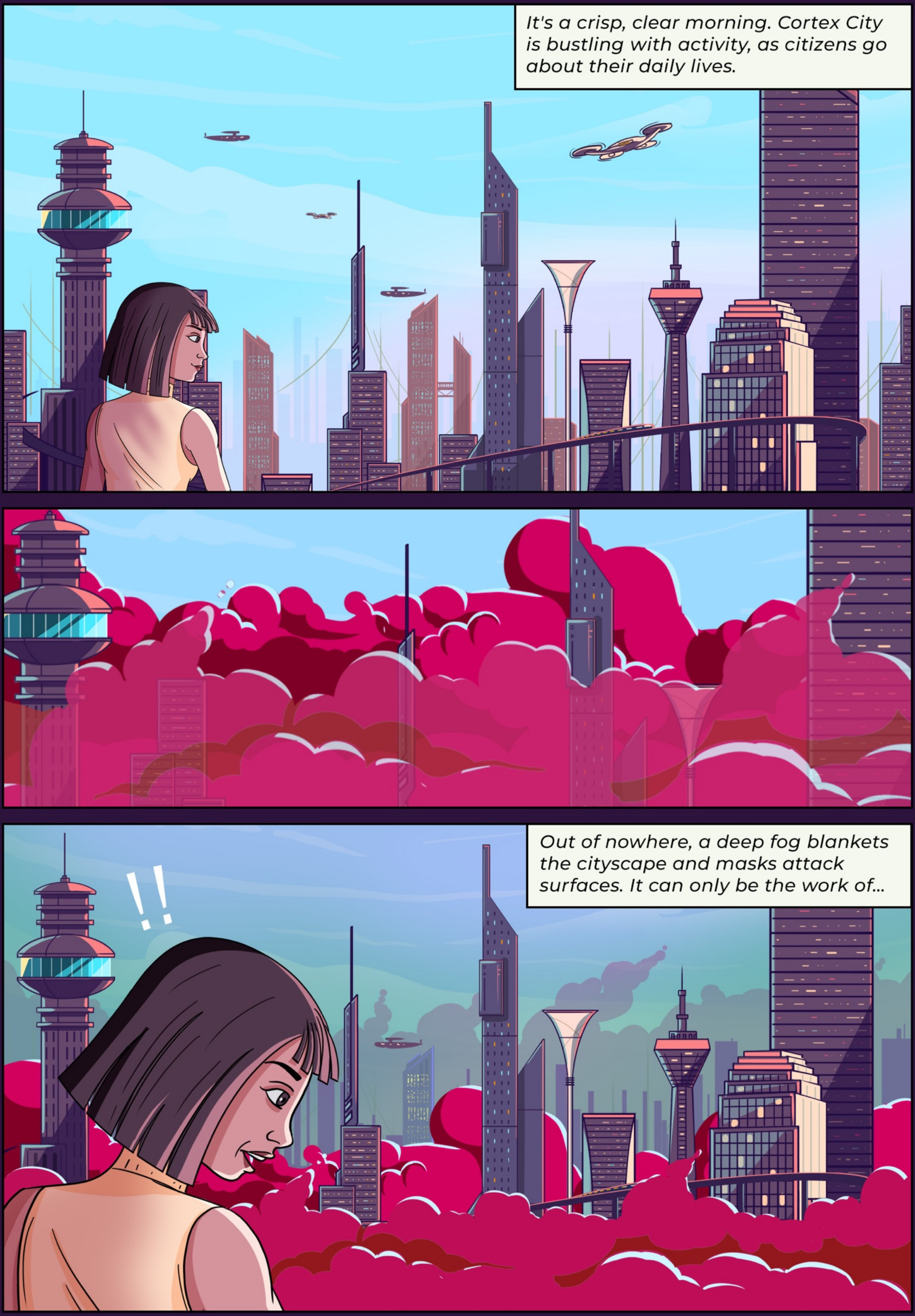
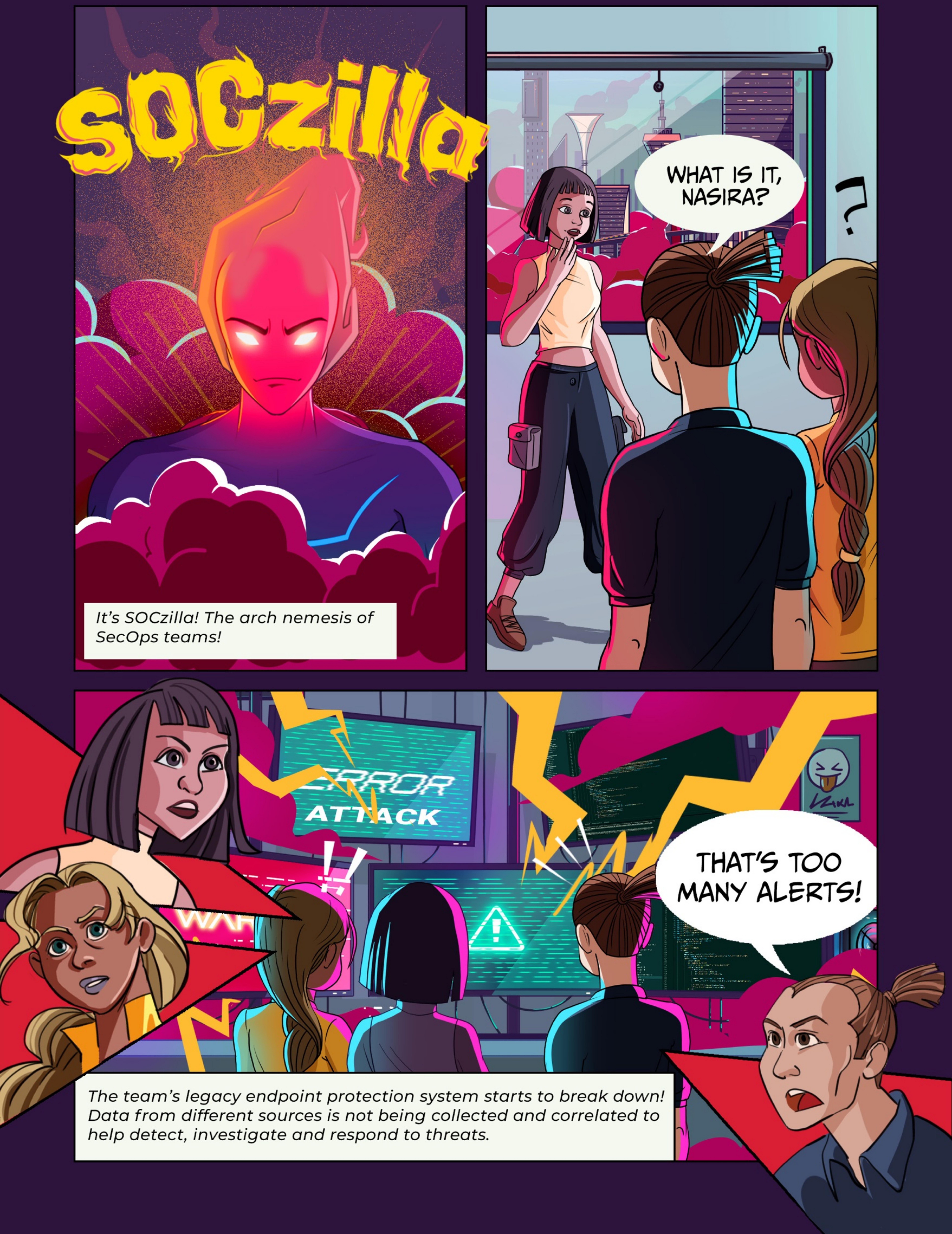
paloalto® NETWORKS | CORTEX® BY PALO ALTO NETWORKS

CORTEX CITY

SOCZILLA VS FUTURESOC

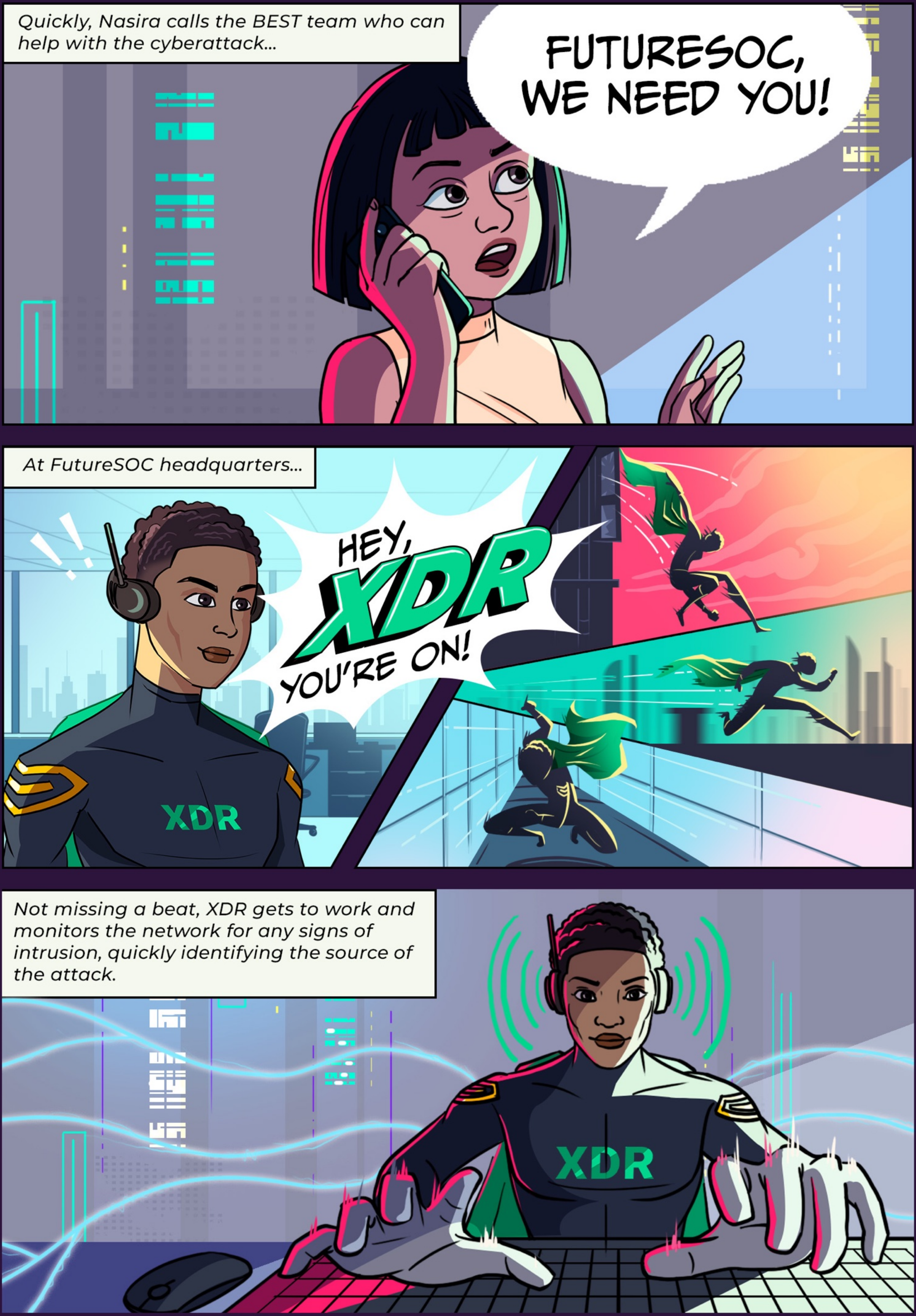
ISSUE #01

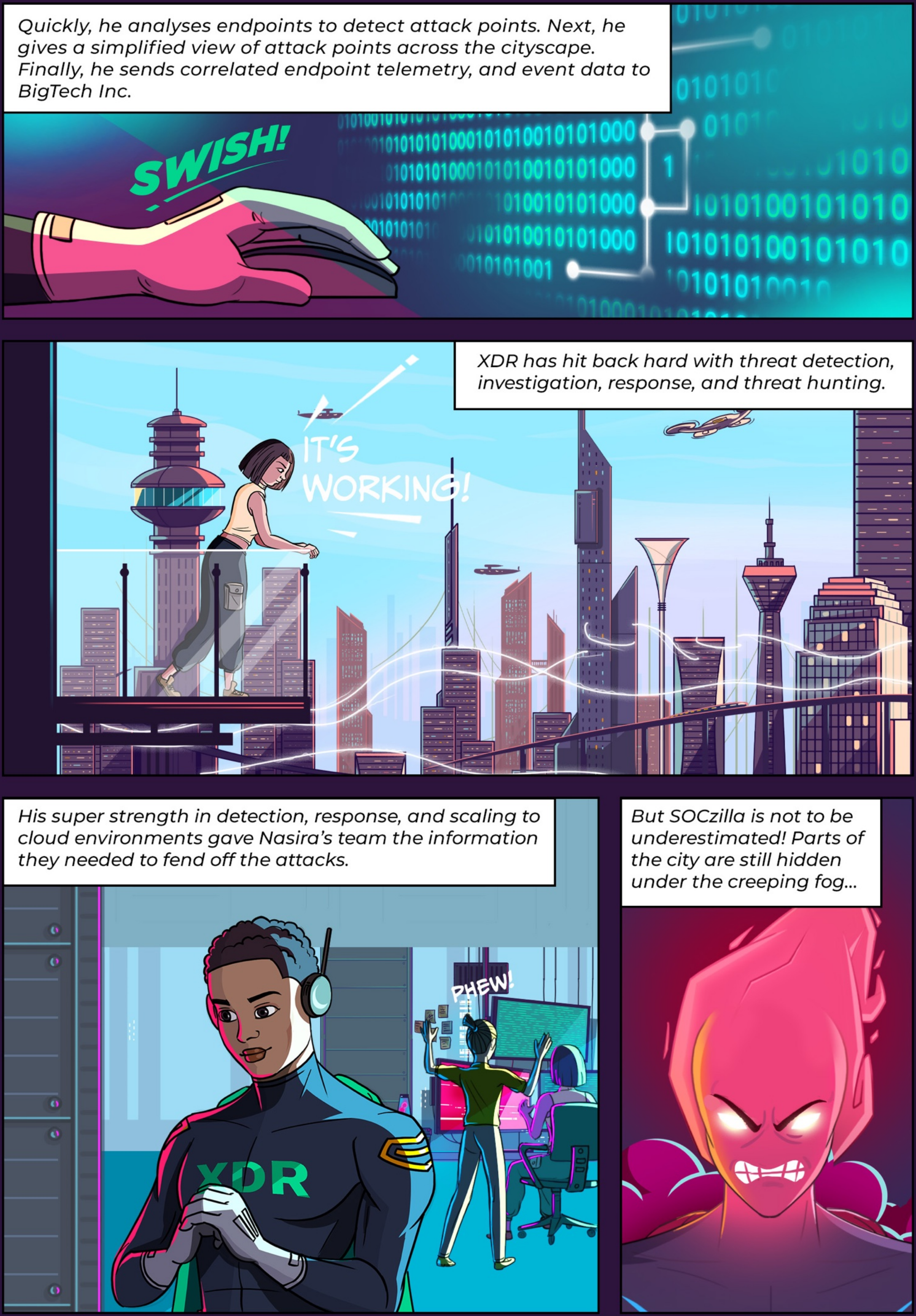

It's a crisp, clear morning. Cortex City is bustling with activity, as citizens go about their daily lives.
Out of nowhere, a deep fog blankets the cityscape and masks attack surfaces. It can only be the work of...
!!



It's SOCzilla! The arch nemesis of SecOps teams!

The team's legacy endpoint protection system starts to break down! Data from different sources is not being collected and correlated to help detect, investigate and respond to threats.


Quickly, Nasira calls the BEST team who can help with the cyberattack...
FUTURESOC, WE NEED YOU!
At FutureSOC headquarters...
HEY, XDR YOU'RE ON!
XDR
Not missing a beat, XDR gets to work and monitors the network for any signs of intrusion, quickly identifying the source of the attack.
XDR



Quickly, he analyses endpoints to detect attack points. Next, he gives a simplified view of attack points across the cityscape. Finally, he sends correlated endpoint telemetry, and event data to BigTech Inc.

XDR has hit back hard with threat detection, investigation, response, and threat hunting.

His super strength in detection, response, and scaling to cloud environments gave Nasira's team the information they needed to fend off the attacks.

But SOCzilla is not to be underestimated! Parts of the city are still hidden under the creeping fog...

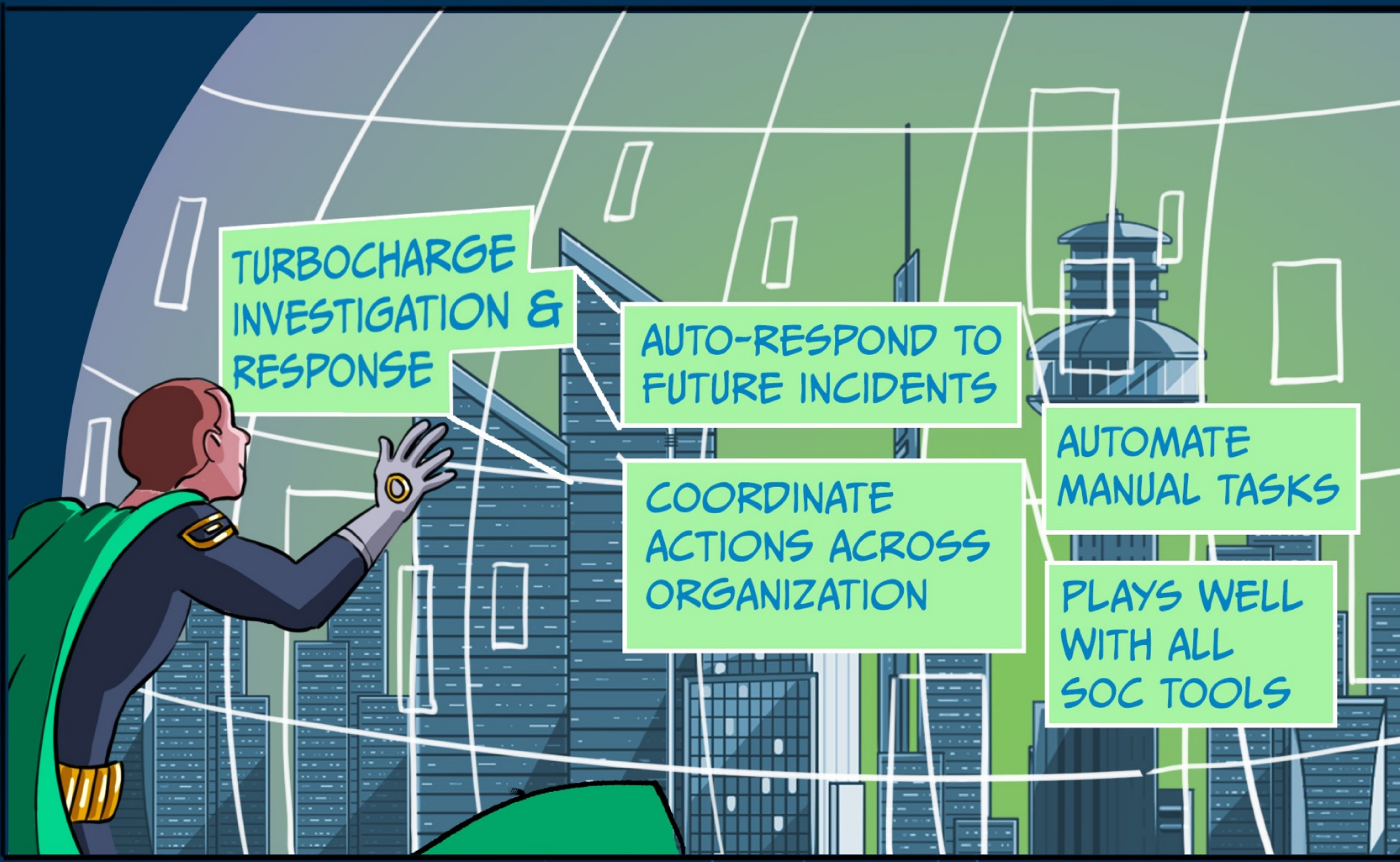
Nasira and XDR call the FutureSOC team for greater protection.

LET'S PROTECT BIGTECH INC.!
WE'RE ON OUR WAY!
BLEEP!
XPANSE

Xpanse finds vulnerabilities before SOCzilla can. She continuously discovers assets and monitors them, mitigating risks proactively. She cross-correlates her view of assets with outside-in mapping and then...

XPANSE VISION
16:45:00

She absorbs all the information to understand exposure to new attacks and how attacks have unfolded. The fog is almost eradicated!
Xpanse
XSOAR arrives to help Xpanse finish the job!
XSOAR
Xpanse
XSOAR


TURBOCHARGE INVESTIGATION & RESPONSE
AUTO-RESPOND TO FUTURE INCIDENTS
AUTOMATE MANUAL TASKS
COORDINATE ACTIONS ACROSS ORGANIZATION
PLAYS WELL WITH ALL SOC TOOLS

In a flash, XSOAR pulls in alerts from Nasira's tools so he has access to information about endpoints, users, hosts, vulnerabilities, malware and attacker intel to perform immediate containment.

XSOAR takes down the fog! The entire attack surface is finally reduced and cleared to give Nasira and her team a complete view!

With SOCzilla's attacks rebuffed and peace restored, XSOAR shows Nasira and her team how to add automation to their arsenal to thwart supply chain, nation-state and zero-day attacks.

The FutureSOC team helps Nasira's team prioritize their incoming alerts and streamline their workflows to speed up remediation through AI and machine learning.

The secret to their success was Cortex's comprehensive product suite. With endpoint security, detection, response, automation and attack surface management, Nasira and the team spend less time on busywork and even reclaimed their nights and weekends!

IN THE END

With one single source of truth for network, cloud and identity data as well as Internet-exposed asset risk to accurately detect threats, Nasira and her team can spot even the most stealthy SOCzilla attack and respond with the full force of the SOC.

The FutureSOC team proved that with the right security technologies, even the most advanced of SOCzilla's threats can be defeated.

By having full visibility and a coordinated response to security incidents, you too can proactively defend and protect networks and assets for a rosy future.

Start the journey to your SOC of the future to meet the shifting demands of a cloud-native world with Cortex today. Click here to request for a demo!