uptycs

# THE UNIFIER

ISSUE

1

AUG 2023

## KEEPING THE WORLD SAFE FROM CYBER ATTACKS

Story and production by
**John Papageorge**
Art by **Kikue Yamazaki**

# Why industry leaders choose Uptycs.

"I would not want to do security anywhere without this **level of visibility**."

sel

"We've gotten a **significant ROI** on our Uptycs investment by playing to its strengths – the single data model and backend analytics."

Lookout

"It's a **single solution** where we can correlate data from user endpoints and cloud."

CROSSBEAM

Uptycs was deployed on a **large scale** as a key component of our security posture."

COMCAST

"Uptycs contextualizes threat activity across K8s, cloud services, and laptops. We've **dramatically shortened** our threat investigation time."

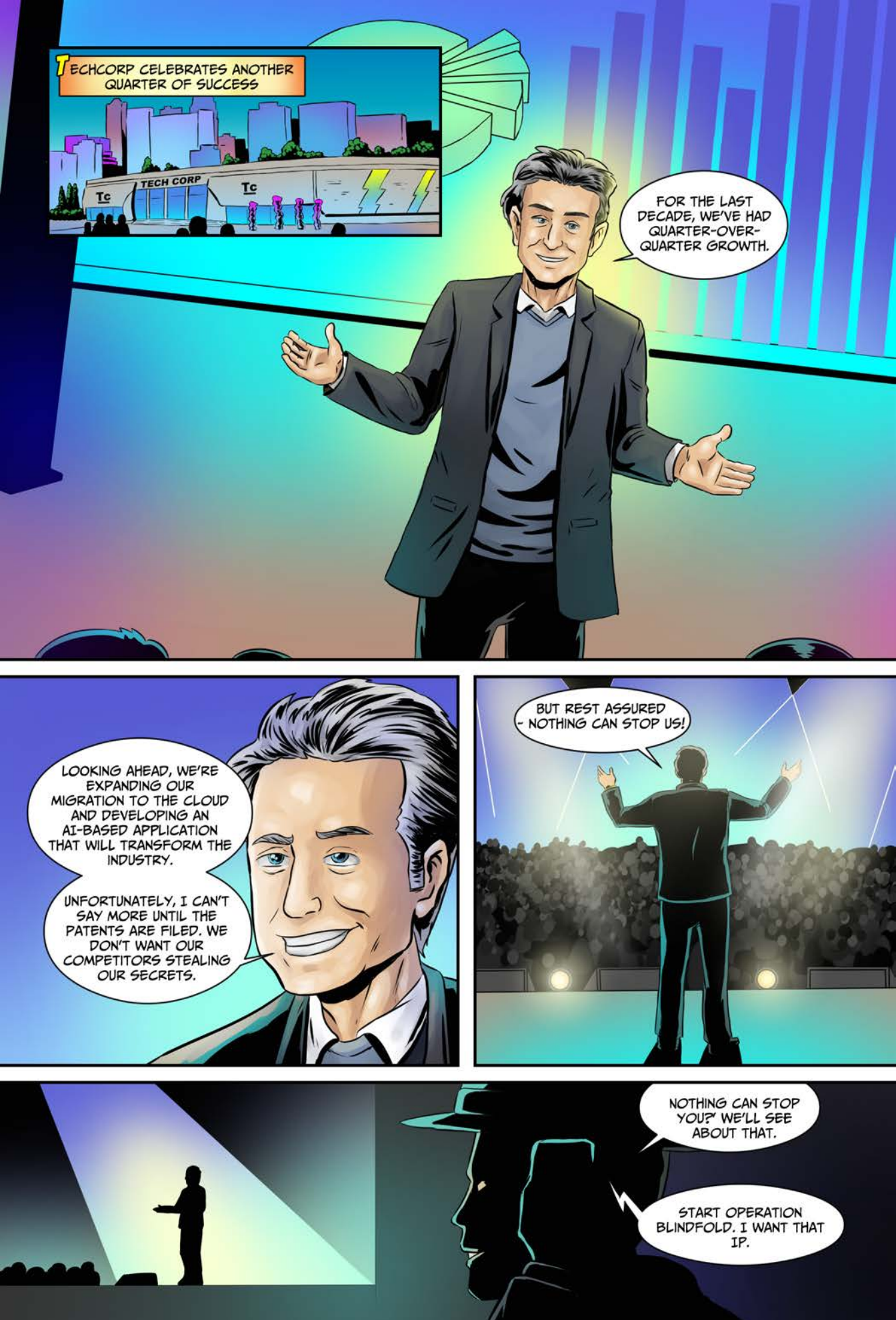
GREENLIGHT

## About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across clouds, containers, servers, and endpoints—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive enterprise-wide security posture. Get started with agentless coverage, then add runtime protection and advanced remediation and forensics.

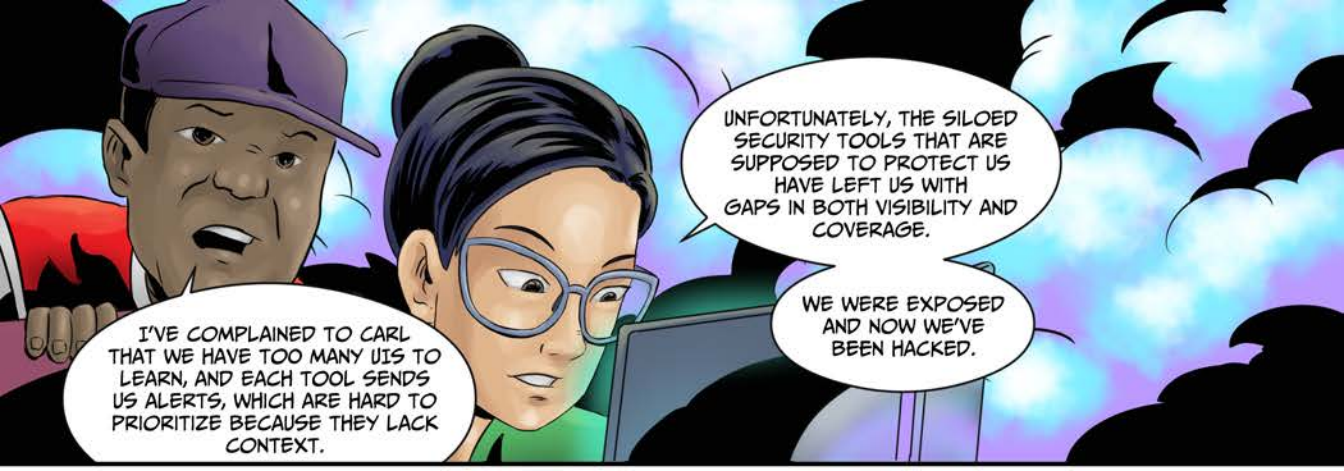
**Shift up your cybersecurity with Uptycs.**

uptycs


TECHCORP CELEBRATES ANOTHER QUARTER OF SUCCESS
TECH CORP
FOR THE LAST DECADE, WE'VE HAD QUARTER-OVER-QUARTER GROWTH.
LOOKING AHEAD, WE'RE EXPANDING OUR MIGRATION TO THE CLOUD AND DEVELOPING AN AI-BASED APPLICATION THAT WILL TRANSFORM THE INDUSTRY.
UNFORTUNATELY, I CAN'T SAY MORE UNTIL THE PATENTS ARE FILED. WE DON'T WANT OUR COMPETITORS STEALING OUR SECRETS.
BUT REST ASSURED - NOTHING CAN STOP US!
NOTHING CAN STOP YOU?' WE'LL SEE ABOUT THAT.
START OPERATION BLINDFOLD. I WANT THAT IP.

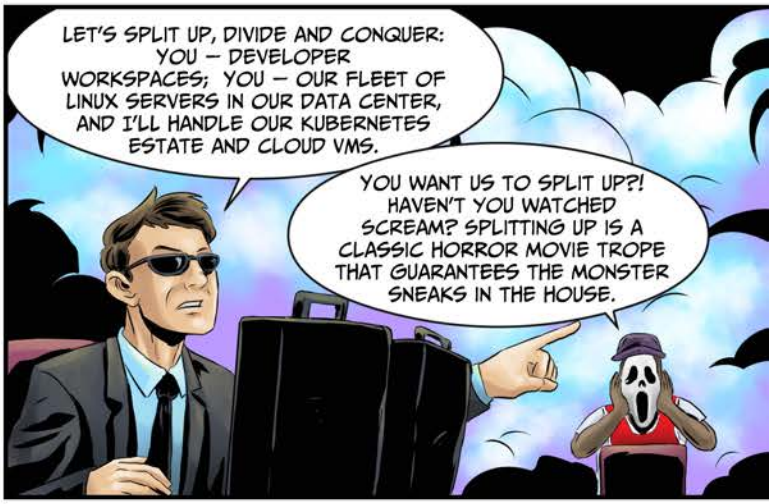

MEANWHILE... TECHCORP'S SECURITY TEAM WELCOMES A NEW TEAM MEMBER.
SAMANTHA, I'D LIKE TO INTRODUCE YOU TO DAVID, HE WORKS REMOTELY, DEVELOPING OUR CLOUD APPS AND DEPLOYING THEM USING KUBERNETES.
THERE'S ALSO STEVEN IN DEVSECOPS. AND, OF COURSE, ALBERT IS OUR APPSEC SPECIALIST AND RESIDENT CINEPHILE.
WELCOME TO THE REAL WORLD. IT SUCKS. YOU'RE GONNA LOVE IT.
I'M GLAD TO BE HERE.
I'LL LET YOU ALL GET BACK TO WORK. 'THE FATE OF THE UNIVERSE IS IN YOUR HANDS'.
GUARDIANS OF THE GALAXY.


JUST AT THAT MOMENT
WHAT'S GOING ON? I CAN'T SEE ANYTHING ON MY SCREEN.
ME NEITHER.
TEAM, CAN YOU HEAR ME? HELP! I THINK I'VE BEEN HACKED.
DAVID, I CAN'T SEE THE SEQUENCE OF SECURITY EVENTS THAT LED TO THIS – THESE SILOED SECURITY TOOLS HAVE IMPEDED OUR VISIBILITY.
THIS IS LIKE JOHN CARPENTER'S 1980'S HORROR CLASSIC THE FOG. WEATHER FORECAST: EXPECT A HIGH CHANCE OF CYBER ATTACKS FOLLOWED BY A CORPORATE STORM.
I BELIEVE THE ATTACKER MAY HAVE MOVED LATERALLY FROM DAVE'S LAPTOP INTO OUR CLOUD. BUT HOW'D THEY GET THE ACCESS TOKEN? HERE, I'M SEEING SIGNS OF UNAUTHORIZED ACCESS AND UNUSUAL USER ACTIVITY ON DAVE'S LAPTOP, BUT IT'S HARD TO CONNECT THE DOTS ON WHERE THE ATTACKER WENT FROM THERE.
SAMANTHA, WHAT SHOULD WE DO?

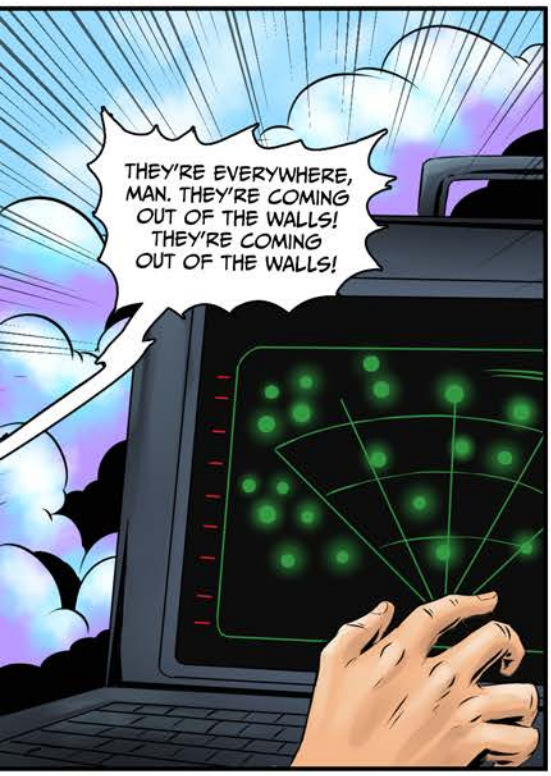

I'VE COMPLAINED TO CARL THAT WE HAVE TOO MANY UIS TO LEARN, AND EACH TOOL SENDS US ALERTS, WHICH ARE HARD TO PRIORITIZE BECAUSE THEY LACK CONTEXT.
UNFORTUNATELY, THE SILOED SECURITY TOOLS THAT ARE SUPPOSED TO PROTECT US HAVE LEFT US WITH GAPS IN BOTH VISIBILITY AND COVERAGE.
WE WERE EXPOSED AND NOW WE'VE BEEN HACKED.


AT THAT MOMENT...


LET THE SILO SPECIALISTS TAKE OVER.
FRANKLY, IT WAS YOUR SILOED SECURITY TOOLS THAT GOT US IN THIS TROUBLE.


LET'S SPLIT UP, DIVIDE AND CONQUER: YOU – DEVELOPER WORKSPACES; YOU – OUR FLEET OF LINUX SERVERS IN OUR DATA CENTER, AND I'LL HANDLE OUR KUBERNETES ESTATE AND CLOUD VMS.
YOU WANT US TO SPLIT UP?! HAVEN'T YOU WATCHED SCREAM? SPLITTING UP IS A CLASSIC HORROR MOVIE TROPE THAT GUARANTEES THE MONSTER SNEAKS IN THE HOUSE.


GEEZ, I'M NOT A FAN OF THIS GUY!

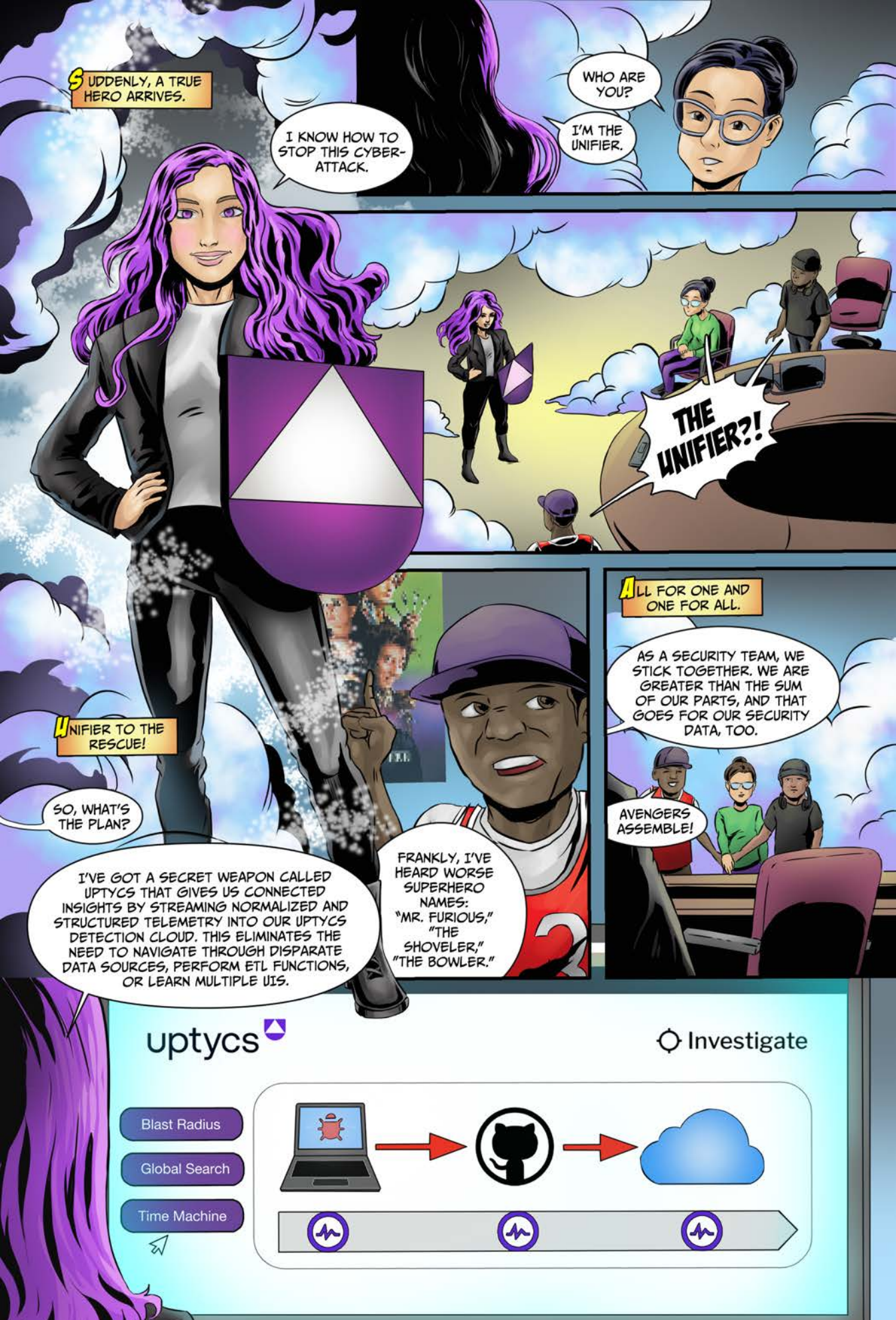

THEY'RE EVERYWHERE, MAN. THEY'RE COMING OUT OF THE WALLS! THEY'RE COMING OUT OF THE WALLS!

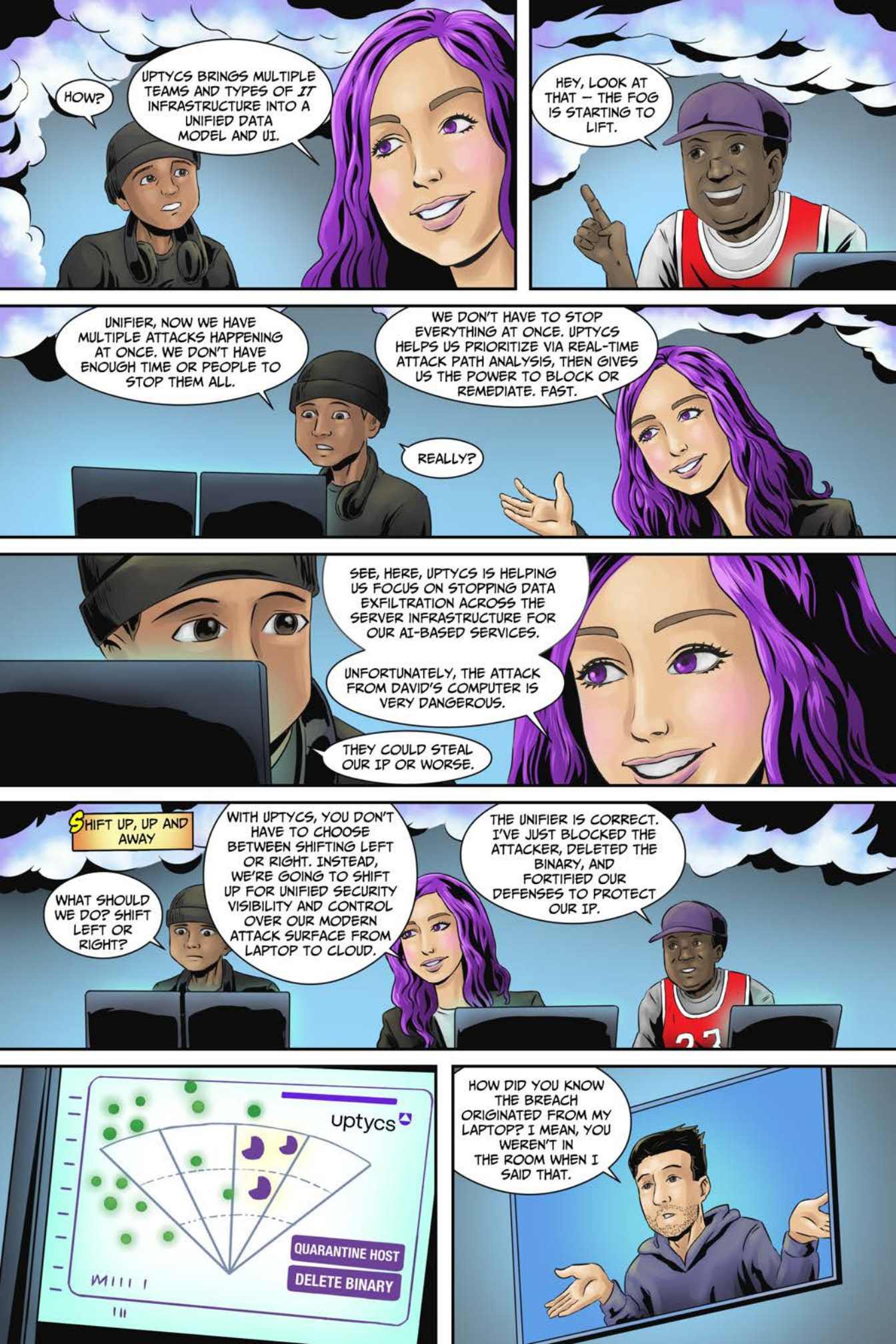

DID YOU JUST QUOTE JAMES CAMERON'S 1982 CLASSIC FILM 'ALIENS?'


THEY'RE ATTACKING FROM ALL SIDES. FALL BACK! FALL BACK!


FOLLOWED BY A CHEAP JON SNOW REFERENCE.


THERE ARE TOO MANY GAPS, TOO MANY HOLES. LET'S GET OUT OF HERE!


SUDDENLY, A TRUE HERO ARRIVES.
I KNOW HOW TO STOP THIS CYBER-ATTACK.
WHO ARE YOU?
I'M THE UNIFIER.
THE UNIFIER?!
UNIFIER TO THE RESCUE!
SO, WHAT'S THE PLAN?
I'VE GOT A SECRET WEAPON CALLED UPTYCS THAT GIVES US CONNECTED INSIGHTS BY STREAMING NORMALIZED AND STRUCTURED TELEMETRY INTO OUR UPTYCS DETECTION CLOUD. THIS ELIMINATES THE NEED TO NAVIGATE THROUGH DISPARATE DATA SOURCES, PERFORM ETL FUNCTIONS, OR LEARN MULTIPLE UIS.
FRANKLY, I'VE HEARD WORSE SUPERHERO NAMES: "MR. FURIOUS," "THE SHOVELER," "THE BOWLER."
F.B.I.
ALL FOR ONE AND ONE FOR ALL.
AS A SECURITY TEAM, WE STICK TOGETHER. WE ARE GREATER THAN THE SUM OF OUR PARTS, AND THAT GOES FOR OUR SECURITY DATA, TOO.
AVENGERS ASSEMBLE!
uptycs
Investigate
Blast Radius
Global Search
Time Machine


HOW?
UPTYCS BRINGS MULTIPLE TEAMS AND TYPES OF IT INFRASTRUCTURE INTO A UNIFIED DATA MODEL AND UI.
HEY, LOOK AT THAT — THE FOG IS STARTING TO LIFT.
UNIFIER, NOW WE HAVE MULTIPLE ATTACKS HAPPENING AT ONCE. WE DON'T HAVE ENOUGH TIME OR PEOPLE TO STOP THEM ALL.
WE DON'T HAVE TO STOP EVERYTHING AT ONCE. UPTYCS HELPS US PRIORITIZE VIA REAL-TIME ATTACK PATH ANALYSIS, THEN GIVES US THE POWER TO BLOCK OR REMEDIATE. FAST.
REALLY?
SEE, HERE, UPTYCS IS HELPING US FOCUS ON STOPPING DATA EXFILTRATION ACROSS THE SERVER INFRASTRUCTURE FOR OUR AI-BASED SERVICES.
UNFORTUNATELY, THE ATTACK FROM DAVID'S COMPUTER IS VERY DANGEROUS.
THEY COULD STEAL OUR IP OR WORSE.
SHIFT UP, UP AND AWAY
WHAT SHOULD WE DO? SHIFT LEFT OR RIGHT?
WITH UPTYCS, YOU DON'T HAVE TO CHOOSE BETWEEN SHIFTING LEFT OR RIGHT. INSTEAD, WE'RE GOING TO SHIFT UP FOR UNIFIED SECURITY VISIBILITY AND CONTROL OVER OUR MODERN ATTACK SURFACE FROM LAPTOP TO CLOUD.
THE UNIFIER IS CORRECT. I'VE JUST BLOCKED THE ATTACKER, DELETED THE BINARY, AND FORTIFIED OUR DEFENSES TO PROTECT OUR IP.
uptycs
QUARANTINE HOST
DELETE BINARY
HOW DID YOU KNOW THE BREACH ORIGINATED FROM MY LAPTOP? I MEAN, YOU WEREN'T IN THE ROOM WHEN I SAID THAT.


THE REASON I KNEW IS UPTYCS TIES TOGETHER ATTACK ACTIVITY AS IT TRAVERSES ON-PREM AND CLOUD BOUNDARIES TO MITIGATE RISK ASSOCIATED WITH CYBERCRIME.
IT'S LIKE WITH UPTYCS, WE HAVE THE EYE OF SAURON, AN ALL-ENCOMPASSING GAZE WHERE NO ATTACK ESCAPES OUR ATTENTION.
UPTYCS BRIDGES THE GAP BETWEEN DEVELOPMENT, SECURITY, AND OPERATIONS TEAMS BY UNITING TOOLING AND SECURITY PROCESSES.
IT ALSO ELIMINATED THE NEED TO LEARN SEPARATE UIS, ADMINISTER MULTIPLE POLICY ADMIN POINTS, AND MAINTAIN NUMEROUS AD HOC INTEGRATIONS.
AND GOT RID OF THE NEED FOR THOSE COSTLY, INEFFECTIVE SILO SPECIALISTS THAT KEPT DIVIDING US.
I HEARD THE NEWS. YOU STOPPED THE BAD ACTORS.
AND WHEN YOU SAY BAD ACTORS, I ASSUME YOU DON'T MEAN STEVEN SEAGAL.
BUT SERIOUSLY, HOW WERE YOU ALL ABLE TO ACCURATELY IDENTIFY THE ATTACK AND CONTAIN IT SO QUICKLY?
UPTYCS!
MEANWHILE, IN A DARK CAVERNOUS HIDEOUT.
OPERATION BLINDFOLD WAS A FAILURE.
HOW? YOU SAID THEIR SILOED SECURITY SYSTEMS WOULD BE EASY TO INFILTRATE AND GET THAT IP OR AT LEAST GET THEIR CUSTOMER DATA.
THEY KNEW WE WERE COMING.
THEY CAN SEE OUR SUSPICIOUS ACTIVITY AND APPEAR TO ZERO IN ON US WHENEVER WE APPROACH CROWN JEWEL DATA. THEY CUT OFF OUR ABILITY TO EXPLOIT A WEAKNESS IN ONE AREA TO MOVE TO AN ADJACENT AREA TO GET TO THAT IP. THEY CUT US OFF.
HOW COULD THEY HAVE DONE SUCH FAST, ACCURATE, THREAT DETECTION AND RESPONSE. HOW?!
UPTYCS.


uptycs.com