

# XDR vs EXPLOIT0

A TECHSLAYER CHRONICLES ADVENTURE



ActualTech  
MEDIA

BROUGHT TO YOU BY:

RAPID7

# **XDR vs Exploito**

## **A Techslayer Chronicles Adventure**

Copyright © 2022 by ActualTech Media

All rights reserved. This book or any portion may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

ActualTech Media

6650 Rivers Avenue Ste 105 #22489  
North Charleston, South Carolina  
29406-4829

[www.actualtechmedia.com](http://www.actualtechmedia.com)

### **Acknowledgements**

Author  
**Scott D. Lowe**

Scott D. Lowe is the CEO and Lead Analyst for ActualTech Media. Since 1994, Scott has helped organizations of all types solve critical technology challenges. He has served in a variety of technical roles, spent ten years as a CIO, and has spent another thirteen as a strategic IT consultant in higher education. Today, his company helps educate IT pros and decision makers and brings IT consumers together with the right enterprise IT solutions to help them propel their businesses forward.

Special Contributions From  
**James Green, Partner and VP at ActualTech Media**

Art & Illustration  
**Eric M. Strong**

Editors  
**Keith Ward**  
**Wendy Hernandez**

Senior Director of Content  
**Katie Mohr**



### **About ActualTech Media**

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services. ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience. Our leadership team is stacked with former CIOs, IT Managers, architects, subject matter experts and marketing professionals who help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you are an IT marketer and you'd like your own custom content, please visit us at **[www.actualtechmedia.com](http://www.actualtechmedia.com)**.



YOU'LL NEVER  
GET AWAY WITH  
YOUR EVIL SPEAR  
PHISHING,

**EXPLOITO!**

TOO LATE,  
**CAPTAIN  
CYBER!**

OUTABIZ  
CORP NEVER  
STOOD A  
CHANCE,

THE EMAIL  
FILTERS ARE  
OUT-OF-DATE!

TRAINING IS  
A JOKE, HUMANS  
ARE HUMANS!

THEY WERE  
SITTING DUCKS!





THIS POWERSHELL RULE CAN STOP YOU!



I WILL STOP YOU!

YOU ARE A LOWLY HUMAN CRIME WAVE, EXPLOITO.

YOU'LL WISH YOU HADN'T MET ME!

TOO LATE! THOSE FOOLS AT OUTABIZ SHOULD HAVE RECRUITED YOU SOONER!



DO YOU SERIOUSLY THINK THAT WILL WORK?



I'VE ALREADY TAKEN OVER THE ACCOUNT, ESCALATED MY PRIVILEGES, DONE RECONNAISSANCE.



I'VE BEEN IN THE NETWORK FOR WEEKS!

OUTABIZ CORP PRACTICALLY LEFT THE FRONT DOOR OPEN FOR ME!



BY THE TIME YOU GOT HERE, I WAS A LATERAL MOTION MACHINE, THE ECCLESARCH OF EXFILTRATION. THIS COMPANY BETTER GET READY FOR THE EVENING NEWS. I'VE JUST MADE THEM AS FAMOUS AS I AM!



UNTIL NEXT TIME, CAPTAIN CYBER!



WHY DO YOU DO THIS?

WHY DO YOU DESTROY BUSINESSES AND LIVES?



MONEY! GLORY! SELF-ACTUALIZATION!

WHEN COMPANIES LEAVE THE DOOR OPEN, I GO IN!



THOOM!

CONGLOMOCORP

THE NEXT TARGET MUST BE MORE PREPARED FOR ATTACKS.

I'LL DITCH MY CAPE, SPANDEX, AND SPIKEY HEEL BOOTS AND I'LL HELP THEM USING MY SECRET IDENTITY: THE MILD-MANNERED CISO, ADIRA ADAMA.



A FEW DAYS LATER...



WELCOME TO  
CONGLOMOCORP!



YOUR CREDENTIALS ARE  
IMPRESSIVE, ADIRA. WE'RE  
EAGER TO HAVE YOU  
PROTECT THE COMPANY AS  
OUR VERY FIRST CHIEF  
INFORMATION SECURITY  
OFFICER.

THANK YOU. I'M  
CONFIDENT MY TEAM  
AND I CAN KEEP  
CONGLOMOCORP  
SAFE.

OR CAN THEY?

EXPOITO WAS RUNNING A PORT SCAN IN STROBE  
MODE SO AS TO NOT TRIGGER AN ALERT.  
MEANWHILE, SECURITY WAS DISTRACTED BY  
FALSE ALARMS.

JOSH WAS ON EDGE (AND THAT'S NO PLACE TO  
BE). HE DIDN'T WANT TO SEEM PANICKY AROUND  
THE NEW BOSS, BUT HEY: HE WAS PANICKED.



WE'VE GOT  
BAD BOTS!



LET'S START WITH MORE  
LIKELY THINGS, JOSH. HAVE  
YOU CHECKED FOR  
MISCONFIGURATIONS? LIKE  
SAVED PASSWORDS THAT  
AREN'T UPDATED WHEN THE  
PASSWORD IS RESET FOR  
SERVICE ACCOUNTS?

OR MAYBE  
DISCONNECTED  
SESSIONS THAT ARE  
STILL ATTEMPTING TO  
AUTHENTICATE?



THIS LOOKS  
BAD! BETTER  
TELL ADIRA...



I'M SEEING  
ANOMALOUS TRAFFIC AND  
GETTING BRUTE FORCE  
ALERTS! IT HAS TO BE BAD  
BOTS! WE'RE GETTING  
HACKED!



WELL, NO...





HEY ADIRA,  
I THINK THE CFO  
GOT PHISHED.

BUT ENDPOINT  
PROTECTION  
WOULDN'T MISS THAT.  
IT'S ON EVERYONE'S  
LAPTOPS!



HE WAS  
WORKING AT HOME,  
I KNOW HE JUST  
USES HIS PERSONAL  
LAPTOP SOMETIMES,  
SO...



...OR, WHO  
KNOWS, THERE'S  
BEEN A FILTERING  
PROBLEM. LOTS OF  
FALSE POSITIVES,  
SO WE DON'T JUMP  
AT EVERY SINGLE  
ONE...



BY THE WAY,  
YOU JUST GOT  
HERE BUT I'M  
LEAVING.

NEW  
JOBS FOR  
EVERYBODY,  
HUH?



BUT YOU'RE  
THE ONE WHO ASSEMBLED  
OUR MAZE OF 45 DIFFERENT  
SECURITY TOOLS. THEY'RE  
FRAGMENTED, WE NEED TO  
MAKE BIG CHANGES, BUT TO  
STREAMLINE I DO NEED  
YOU AROUND!



YOU'LL BE FINE.  
EVERYTHING I DID  
WAS KINDA OBVIOUS,  
YOU'LL SEE.  
GOOD LUCK!



SHUT THE  
NETWORK  
DOWN!



SORRY TO  
WRECK YOUR WORKOUT,  
ADIRA, BUT I THINK WE'RE  
UNDER ATTACK. KEVIN  
LEFT YESTERDAY, AND  
WE'VE BEEN GETTING  
A BONKERS NUMBER  
OF ALERTS.



THEY'RE  
IRRELEVANT, JOSE.  
KEVIN TOLD ME HE DEALT  
WITH THIS NONSENSE  
MANUALLY ON A SYSTEM  
ONLY HE UNDERSTOOD.  
WE NEED DETECTIONS  
THAT ARE REAL AND  
ACTIONABLE.

WHEN WE  
ALL MEET THIS  
AFTERNOON, I'LL  
TELL YOU ABOUT THE  
BIG CHANGES WE'RE  
GOING TO MAKE.

OUR SECURITY  
PROGRAM HAS TO  
BE BETTER.

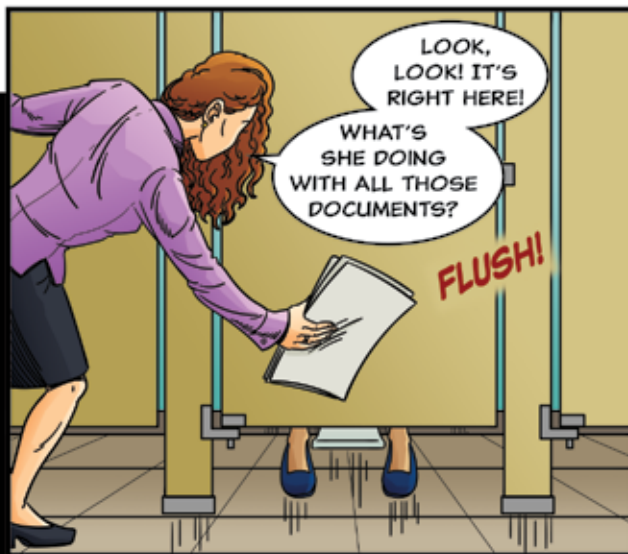
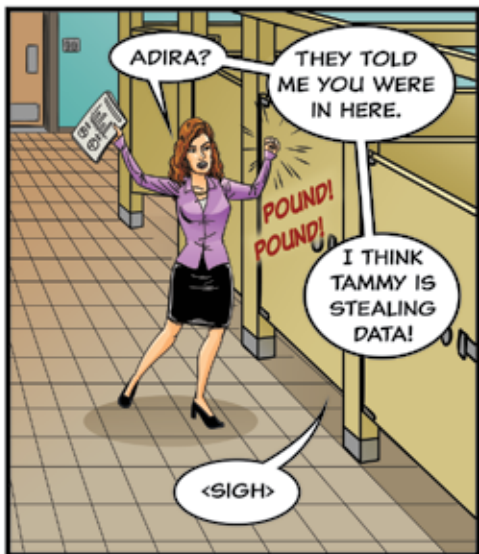


THAT'S GOOD  
TO KNOW, ADIRA. WE  
ALL HAVE ALERT  
FATIGUE.

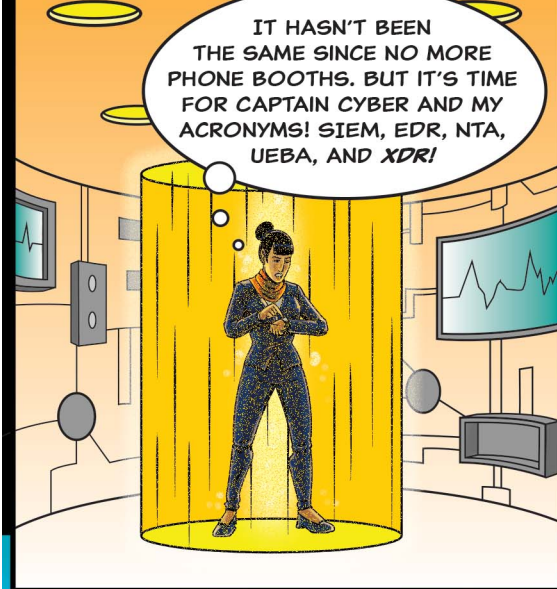


WHO AM I  
KIDDING? FATIGUE?  
IT'S BURNOUT.  
I SHOULD  
JUST GO DELIVER  
PIZZAS.









IT HASN'T BEEN THE SAME SINCE NO MORE PHONE BOOTHS. BUT IT'S TIME FOR CAPTAIN CYBER AND MY ACRONYMS! SIEM, EDR, NTA, UEBA, AND XDR!



I'LL ENTER THE CONGLOMOCORP NETWORK AND SEE WHAT'S GOING ON.

TAKE THAT!



THAT'S JOSH!

HE'S HOLDING HIS OWN, BUT HE KILLS A PROCESS AND IT JUST RESPAWNS!

HOW MUCH LONGER CAN HE KEEP IT UP?

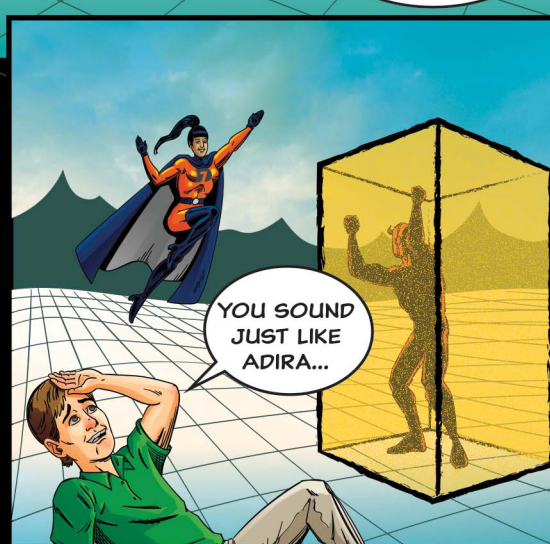
CAPTAIN CYBER!

FOR REAL? I WAS YOUR LAST HALLOWEEN!



THIS WILL HOLD HIM UNTIL YOUR NEW SECURITY PROGRAM IS IN PLACE.

YOU NEED FULL VISIBILITY INTO YOUR ENTIRE ATTACK SURFACE, A DETECTIONS FIRST XDR APPROACH, AND PLENTY OF AUTOMATION. YOU'LL SEE.



YOU SOUND JUST LIKE ADIRA...



THERE'S JOSE! HE'S LOST IN OUR MAZE OF 45 DIFFERENT SECURITY TOOLS AND CODE!

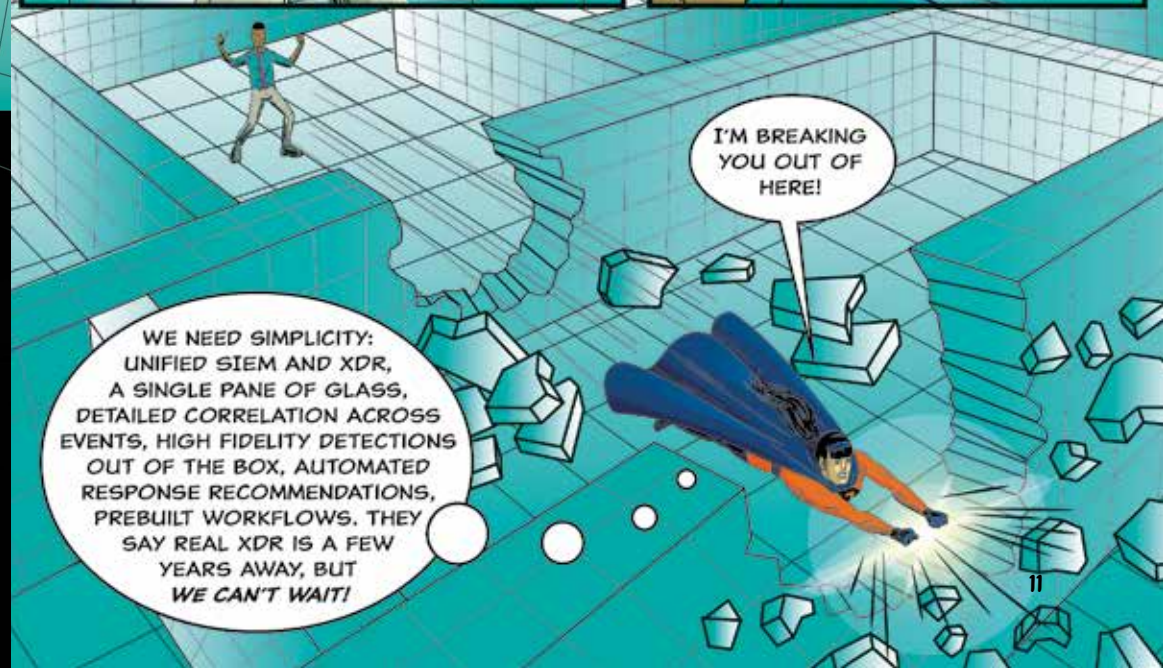


I'LL JUST QUIT AND DELIVER PIZZAS! "MOM? DAD? CAN I BORROW THE CAR? BE FAIR, I BACKED INTO ONE TREE, ONE TIME."

MAYBE IF I WRITE SOME SCRIPTS, SET UP SOME NEW RULES, OUR SYSTEM WILL WORK BETTER. GOTTA THINK LIKE A HACKER AND WRITE MORE CODE!



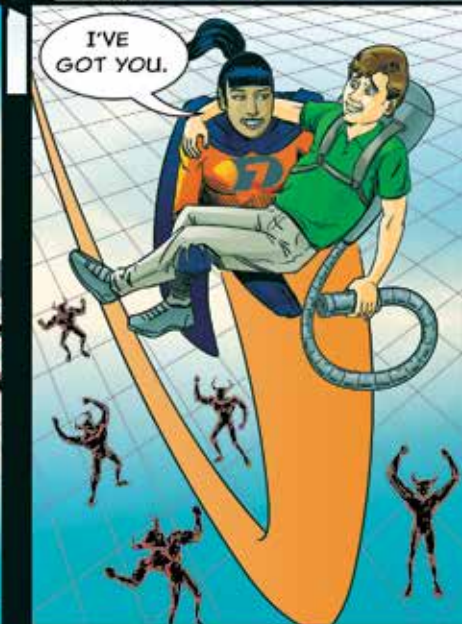
JOSE, MORE CODE CAN'T HELP! THIS ISN'T JUST COMPLEXITY, IT'S LAYERS OF CHAOS!



I'M BREAKING YOU OUT OF HERE!

WE NEED SIMPLICITY: UNIFIED SIEM AND XDR, A SINGLE PANE OF GLASS, DETAILED CORRELATION ACROSS EVENTS, HIGH FIDELITY DETECTIONS OUT OF THE BOX, AUTOMATED RESPONSE RECOMMENDATIONS, PREBUILT WORKFLOWS. THEY SAY REAL XDR IS A FEW YEARS AWAY, BUT WE CAN'T WAIT!









**IT'S A NEW BALLGAME, EXPLOITO.**  
I HAVE RAPID7 INSIGHTIDR.

UNIFIED SIEM AND XDR CAN TAKE YOU DOWN FAST.

MOST SIEMS OUT THERE WERE NOT BUILT TO SUPPORT DETECTION AND RESPONSE FOR TODAY'S MODERN ENVIRONMENTS. BUT INSIGHTIDR WAS. IT'S THE ONLY ONE THAT DELIVERS REAL XDR OUTCOMES: FASTER INSIGHTS, COMPLETE ENVIRONMENT COVERAGE, CURATED DETECTIONS, AND AUTOMATION.

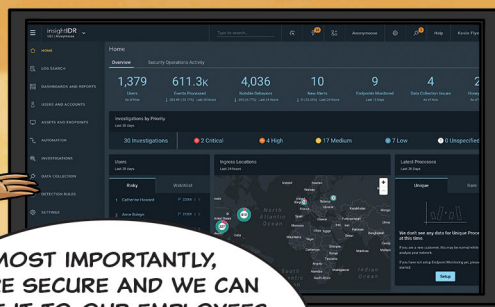
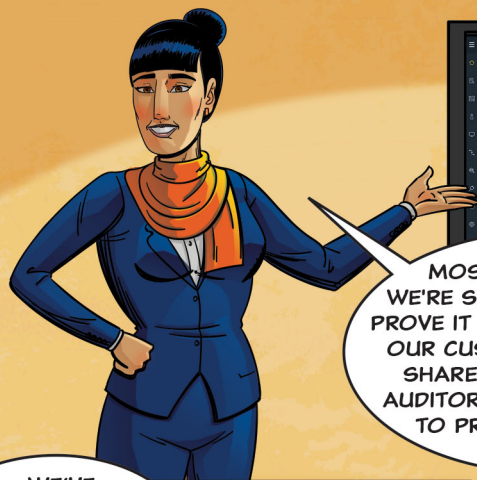
EVIL USED TO WANDER ENVIRONMENTS UNDETECTED FOR DAYS AND DAYS WHILE SECURITY TEAMS SEARCHED LOGS, AND DID CONVOLUTED QUERIES AND DATA SPLUNKING. NO MORE!

NOW, TEAMS CAN ANTICIPATE AND IDENTIFY THREATS EARLY IN THE ATTACK CHAIN. YOU AND YOUR KIND ARE FINISHED, EXPLOITO!









MOST IMPORTANTLY, WE'RE SECURE AND WE CAN PROVE IT TO OUR EMPLOYEES, OUR CUSTOMERS, AND OUR SHAREHOLDERS, AND TO AUDITORS THAT REQUIRE US TO PROVE COMPLIANCE

WE'VE OVERHAULED WHAT WE DISCOVERED TO BE INSECURE SYSTEMS

AND DEPLOYED NEW TOOLS THAT WILL HELP CONGLOMOCORP CONFIDENTLY MEET ITS REVENUE, COMPLIANCE, AND REPUTATION GOALS WITHOUT WORRYING THAT WE'LL FALL VICTIM TO BAD GUYS.

AND OUR SECOPS TEAM IS MORE CONFIDENT AND EFFICIENT. THEY CAN SLEEP AT NIGHT! AND WHEN THEY CAN SLEEP AT NIGHT, YOU FOLKS CAN.

WELL, DONE! CONGLOMOCORP IS SAFER THAN EVER BEFORE!

I COULDN'T HAVE DONE IT WITHOUT MY AMAZING TEAM AND OF COURSE, RAPID7!





# RAPID7

## 5 THINGS YOU NEED IN YOUR NEXT SIEM/XDR

1. CLOUD-BASED. THE FUTURE OF SIEM IS IN THE CLOUD; A CLOUD FOUNDATION WILL HELP -
  - ACCELERATE DEPLOYMENT
  - REQUIRE LESS MAINTENANCE AND OPS WORK FOR THE TEAM
  - SCALE WITH YOUR ENVIRONMENT
  - MAKE IT EASIER TO COLLABORATE ACROSS YOUR TEAM (NO MATTER WHERE IN THE WORLD THEY ARE)
  - PROVIDE THE COMPUTE POWER NECESSARY TO KEEP UP WITH THE MODERN THREAT LANDSCAPE AND ATTACK SURFACE
  - IF YOUR INTERNAL ENVIRONMENT IS COMPROMISED AND YOUR SIEM IS ON-PREM IT, TOO, CAN BE SUBJECT TO ATTACK. HAVING AN "OUT OF BAND" SIEM, MUCH LIKE AN ALTERNATE COMMUNICATION MECHANISM, CAN KEEP YOUR SYSTEMS OPERATIONAL
2. COMPLETE ENVIRONMENT COVERAGE (ACROSS UBA, ENDPOINTS, CLOUD, NETWORK, SECURITY DATA, AND THREAT INTELLIGENCE), FOR ATTACK COVERAGE IN DEPTH, AND TO AVOID CONTEXT SWITCHING AND ACCELERATE INVESTIGATIONS
3. HIGH-FIDELITY OUT-OF-THE-BOX DETECTIONS THAT HELP YOUR TEAM GET UP AND RUNNING QUICKLY (NOT STUCK IN THE WEEDS OF RULE CONFIGURATION, OR RUNNING AROUND DEALING WITH FALSE POSITIVES)
4. CORRELATION AND ATTRIBUTION - THIS IS THE CONNECTIVE TISSUE THAT TIES EVERYTHING TOGETHER AND PROVIDES THE CONTEXT AND INSIGHT THAT MAKE ALERTS ACTIONABLE
5. AUTOMATION-NECESSARY TO UNLOCK THE EFFICIENCY REQUIRED FOR SUCCESSFUL SECURITY OPERATIONS, AND EXTINGUISH THREATS QUICKLY BEFORE THEY BECOME AN ISSUE

