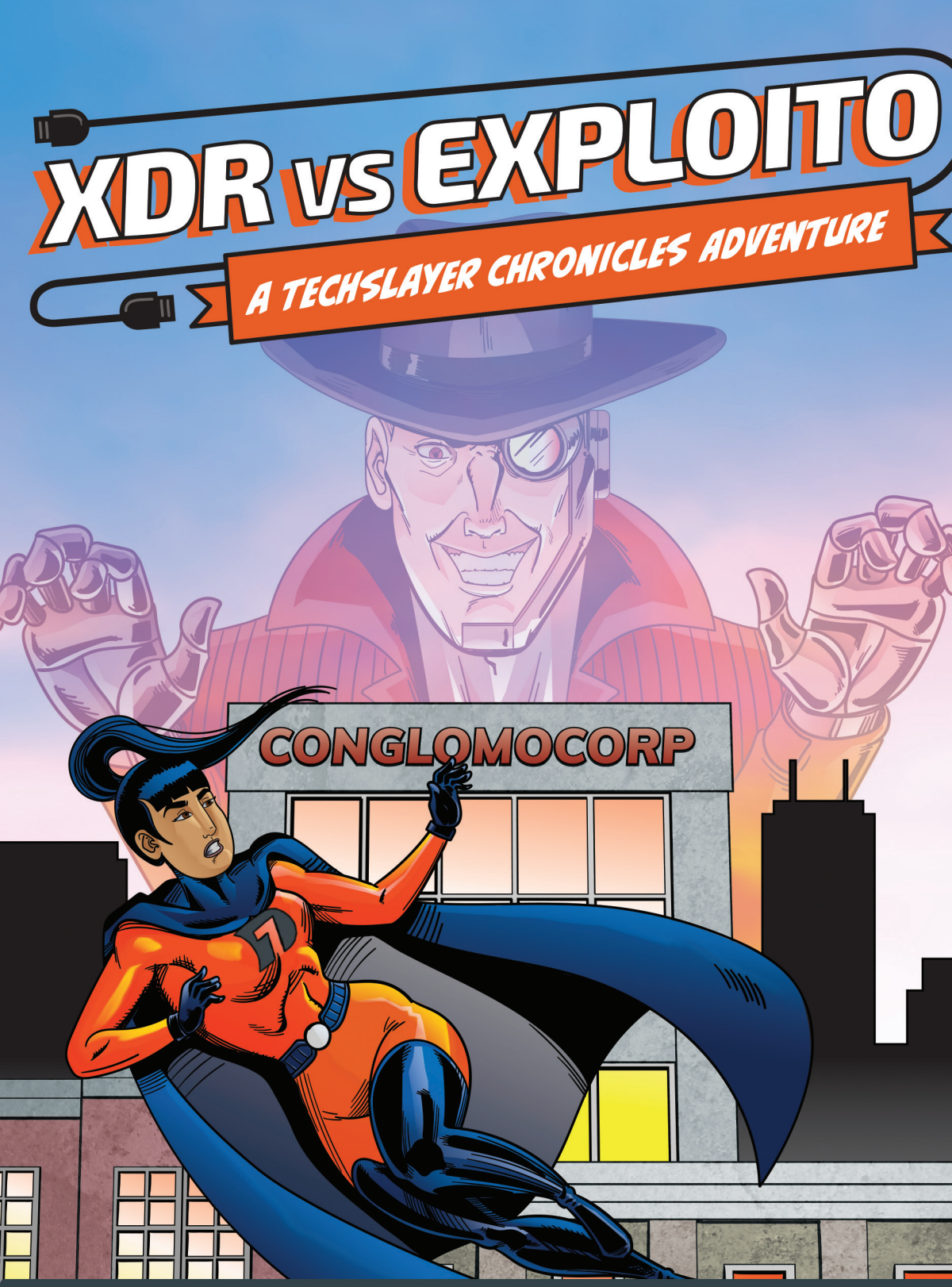
XDR vs EXPLOITO

A TECHSLAYER CHRONICLES ADVENTURE



ActualTech MEDIA

BROUGHT TO YOU BY: RAPID7

The Treatslayer Chronicles

A Techslayer Chronicles Adventure

ActualTech Media

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

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.**


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THE EMAIL FILTERS ARE OUT-OF-DATE!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!
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!
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!


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!
BY THE TIME YOU GOT HERE, I WAS A LATERAL MOTION MACHINE, THE ECCLESIARCH OF EXFILTRATION. THIS COMPANY BETTER GET READY FOR THE EVENING NEWS. I'VE JUST MADE THEM AS FAMOUS AS I AM!
ZZZZZT
UNTIL NEXT TIME, CAPTAIN CYBER!
THOOM!
OUTABIZ
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...
CONGLOMOCORP
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.
THIS LOOKS BAD! BETTER TELL ADIRA...
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!
Josh
I'M SEEING ANOMALOUS TRAFFIC AND GETTING BRUTE FORCE ALERTS! IT HAS TO BE BAD BOTS! WE'RE GETTING HACKED!
Josh
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?
WELL, NO...
5


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.


ADIRA?
THEY TOLD ME YOU WERE IN HERE.
POUND! POUND!
I THINK TAMMY IS STEALING DATA!
<SIGH>
LOOK, LOOK! IT'S RIGHT HERE!
WHAT'S SHE DOING WITH ALL THOSE DOCUMENTS?
FLUSH!
SO YOU'RE A BATHROOM STALKER, EMMA. TERRIFIC!
TAMMY ISN'T STEALING ANYTHING, SHE'S WORKING ON A CLOUD MIGRATION PROJECT.
THIS IS WHY WE DON'T WANT TO BE BLIND TO OUR CLOUD ENVIRONMENT, WHICH WE CURRENTLY ARE. BUT THAT'S GOING TO CHANGE.
OH.
COOL.
WE CAN TALK ABOUT ALL THAT, LIKE, SOMEWHERE ELSE...?
I BETTER HURRY UP. THESE PEOPLE DON'T STAND A CHANCE AGAINST EXPLOITO.


YOU SAID YOU COULD KEEP US SAFE, ADIRA. YOU HAD CONFIDENCE!
CONGLO OCORP
DAILY GAZETTE
CONGLOMOCORP UP IN SMOKE!
CISO TO BLAME
CLOSED DUE TO SECURITY BREACH
SO LONG MILD-MANNERED CISO.
I NEED MY CAPE.


IT HASN'T BEEN THE SAME SINCE NO MORE PHONE BOOTHS. BUT IT'S TIME FOR CAPTAIN CYBER AND MY ACRONYMS! SEIM, 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 YOU 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!*


OH NO! JOSH IS TRYING TO FIGHT OFF EXPLOITO'S MINIONS.
$$$
$$$
$$$
THE COMPANY HAS THROWN MONEY AT THE PROBLEM FOR TOO LONG.THE TRUTH IS, THE MORE TOOLS YOU HAVE THE LESS SAFE YOU ARE!
$$$
BUDGET
I'VE GOT YOU.
LET ME HANDLE IT, JOSH. YOU'LL BE SAFE UP HERE.
I CAN'T HAVE SOLUTIONS THAT EAT UP TOO MUCH CASH AND BURN MONEY.


SOMEONE, HELP!
BOOM!
THAT SOUNDS LIKE EMMA!
THAT LAST EXPLOSIVE DIDN'T WORK.
MAYBE THIS ONE WILL DO THE TRICK!
NMS
OH NO! THAT DIDN'T WORK EITHER.
BOOM!
CAPTAIN CYBER?
THAT WON'T KEEP HIM DOWN FOR LONG! I KNOW YOU'RE HERE, EXPLOITO!
I'M OUT OF TIME, I NEED UNIFIED SIEM AND XDR! FAST!


NO MORE NOISE, COMPLEXITY, TAB HOPPING, AND OPERATIONAL FRICTION.
GIVE ME LIGHTWEIGHT, CLOUD-NATIVE INFRASTRUCTURE WITH SIMPLE SAAS DEPLOYMENT.
GIVE ME DATA INGESTED FROM EVERYWHERE: USER ACTIVITY, LOGS, CLOUD, ENDPOINTS, AND NETWORK TRAFFIC—INTO ONE PLACE.
AND I WANT INSIGHTS!
WHO HAS UNLIMITED BUDGET AND STAFF? WHO CAN WAIT FOR XDR? IT HAS TO BE NOW!
GIVE ME INTERNAL AND EXTERNAL THREAT INTELLIGENCE. I WANT CURATED DETECTIONS! MILLIONS OF DAILY EVENTS SHOULD BE ASSEMBLED INTO ONE PICTURE!
I WANT WIZARD GUIDES AND AUTOMATION! HIGH-CONTEXT INVESTIGATIONS!
GIVE ME RAPID7 INSIGHTIDR!
ALSO, I'D LIKE A MAGICAL POCKET IN MY CAPE LIKE SUPERMAN HAS HAD SINCE 1972! HE KEEPS HIS CLOTHES FOLDED TINY IN THERE.
EVEN HIS SHOES! IN 2006, HE HAD SNACKS IN THERE! COME ON!
THERE'S THE TERMINAL, I KNOW I'LL FIND EXPLOITO THERE.
HE AND HIS MINIONS HAVE HAD FUN PROBING CONGLOMOCORP, BUT IT'S OVER.

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.

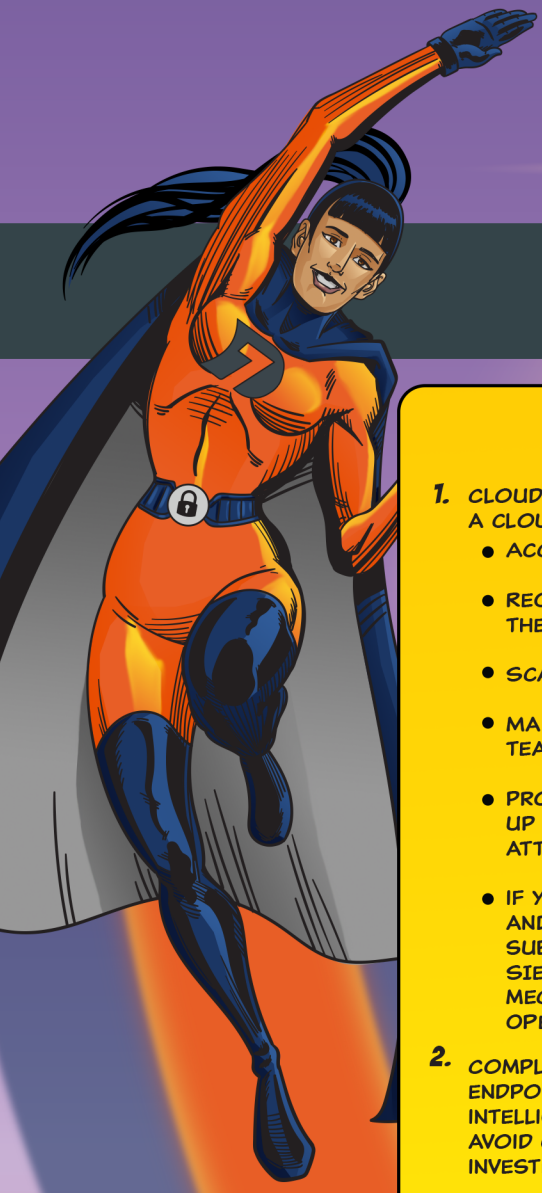
EVIL USED TO WANDER ENVIRONMENTS UNDETECTED FOR DAYS AND DAYS WHILE SECURITY TEAMS SEARCHED LOGS, AND DID CONVOLUTED QUERIES AND DATA SPLUNKING.NO MORE!

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


THIS GIVES MILD-MANNERED CISOS THE ADVANTAGE!
THEY'LL WORK 40-HOUR WEEKS, FOCUS ON WHAT MATTERS MOST, EMPOWER THEIR TEAMS, AND GET THEIR LIVES BACK!
WHAT IS THIS?
I CAN'T MOVE!
AND WITH CISOS IN CONTROL, MAYBE I CAN HANG UP MY CAPE.
I'VE ALWAYS WANTED TO VOLUNTEER IN A PANDA SANCTUARY. UNDERNEATH IT ALL, I'M A CUDDLER.
YOU'RE GOING TO JUST LEAVE ME HERE, AREN'T YOU?


DAYS LATER...
CONGLOM
WITH INSIGHTIDR, WE CONTROL OUR ENTIRE ATTACK SURFACE – ENDPOINTS, CLOUD, NETWORK, USERS – WITH UNIQUE, EMBEDDED THREAT INTELLIGENCE AND A LIBRARY OF DETECTIONS.
DON'T SECURITY PRODUCTS HAVE SLOW DEPLOYMENTS?
MOST DO. BUT INSIGHTIDR IS CLOUD-NATIVE AND SAAS-DELIVERED.
CAN OUR SECURITY TEAM HANDLE THIS SOPHISTICATION?
ABSOLUTELY. IT'S INTUITIVE, ACCESSIBLE, AND VETTED BY RAPID7'S OWN MANAGED SECURITY OPERATIONS AROUND THE WORLD. THEY USE IT FIRST!
IF THAT EVIL EXPLOITO GETS TO US, I'LL BE ON THE EVENING NEWS LOOKING LIKE AN IDIOT. JUST SAYING!
WE WON'T HEAR FROM EXPLOITO AGAIN, SIR.
IN FACT, WE'RE READY TO TANGLE WITH THE RUSSIAN GRU. AND CRAZY STUFF LIKE LOG4SHELL, *DON'T GET ME STARTED ON THAT, SIR.* SERIOUSLY.


Threat Feed Dashboard
1.58k
Assets
with Actively Targeted Vulnerabilities
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

ActualTech Media