CyberMaxx™

Tales from the SOC

Real-world examples that highlight the power of proactive, real-time response.

Threats don't always announce themselves explicitly

Sometimes, they come quietly through a phone call you're not expecting, a subtle change in behavior from one of your colleagues, or a news alert.

That's when **CyberMaxx's "Big R" response** kicks in to help you take real-time action against potential threats.

In this eBook, we've compiled true stories from our Security Operations Center (SOC) that show what is possible when we go beyond detection and into full response to protect our clients from the unseen dangers lurking in their systems.

What Big R Really Means in the SOC

Big R is a mindset that drives every action we take in our Security Operations Center (SOC) here at CyberMaxx.

When we say "Big R," we don't just mean flagging an alert and passing it off to someone else. We're talking about real-time, SOC-led response that races from detection to eradication. That's a sharp contrast to the usual "little r" response, which often stops at a tuned platform and an alert without meaningful follow-through.

Big R means we don't wait until we get a clear-cut alert to make us sure about something. Instead, we act on suspicion. That means if we get a phone call, a notification, or even a hunch from a news feed, we're on it.

Big R vs. Little r: What's the Difference?

Let's break down the differences between typical basic alerting models and CyberMaxx's real-time SOC-led response.

You'll find that traditional alert-based services focus on little things, such as sending alerts without the urgency or action required. That lack of follow-through makes the process both inefficient and unreliable. A notification without a response is just background noise.

In contrast, Big R refers to the response inside the SOC. From the moment we detect something is off, we jump in to authenticate, investigate, and isolate the threat in real time. CyberMaxx compresses the time from incident to eradication without ever handing you off to another team. That approach ensures you're supported throughout and can provide a consistent, cohesive response to threats.

The Power of Acting on Suspicion

At CyberMaxx, we know the worst threats often start as nothing more than a feeling that something's off. It's tempting just to ignore that feeling and wait for a bigger sign.

After all, you don't want to overreact and waste the organization's time and resources, right? Unfortunately, by the time that "bigger sign" actually comes, it's likely that your entire system has already been compromised. The whole reason that Big R shines is that we don't wait for a clear alert to act. If something doesn't feel right, we immediately jump into action.

It could be anything: a phone call from a client, a suspicious post on a forum, or a random feed in the news. Our analysts go straight to work, investigating from every angle. We've already started containing the issue by the time a formal alert comes.

Why a Full Scope of Compromise Is Critical

The first sign of trouble is rarely the full picture, and the initial threat is often just the tip of the iceberg. As a result, the moment we spot something suspicious, we pause and reassess. We ask ourselves, "What else could be happening here?"

With Big R, we look beyond just "A to B" and ask what happens if there's a B.1, B.2, and B.3. This full-scope evaluation ensures we don't miss the threats others might overlook, so we're always one step ahead of attackers.

Here are 5 Tales from the SOC that highlight the power of proactive, real-time response

The Call That Protected Four Clients

One IP Address, Two Organizations Saved

A Malicious Inbox Rule and 300+ Shares

From a Physical Threat to Cyber Defense

A Thumb Drive and a Criminal Investigation

The Call That Protected Four Clients

It all started with a notification from a large enterprise client, who had received a warning from a third-party healthcare provider they support, telling them that the provider had been completely compromised.

Under usual circumstances, our system would have flagged the issue and alerted our team. However, no alert was generated this time. The call alone sparked a chain reaction that revealed risks well beyond the initially compromised provider. CyberMaxx managed to safeguard four clients and prevent further damage by acting proactively.

A Healthcare Provider Sounds the Alarm

A large enterprise client informed us that one of their healthcare clients received a notification from another third-party healthcare provider, saying their systems had been fully compromised. The client was rightfully concerned that the threat group had infiltrated their provider's system, potentially stealing patient data and compromising business records. They wanted to know if it affected them.

Starting with Zero Alerts

The situation didn't follow the usual pattern of being triggered by an alert. CyberMaxx's SOC team was investigating the issue based on that phone call alone. Our analysts authenticated into the client's systems and immediately began manually evaluating potential upstream risks. They conducted a 30-day lookback in search of signs of compromise, but fortunately, there were none.

Proactive Escalation to Other Clients

Even though there were no initial signs of a direct threat to our client, our analysts kept searching. After doing some digging, they realized three other CyberMaxx clients worked with the same healthcare provider. Our team immediately recognized the potential for these other clients to be at risk. Without waiting for confirmation, they proactively investigated each of them, thoroughly assessing their systems for any signs of exposure.

Increased Vigilance and Direct Outreach

Although there was no evidence of a direct compromise, CyberMaxx's analysts didn't take any chances. They elevated monitoring and applied greater vigilance. Even before they were aware of the risk, we notified them that they could potentially be impacted. We simply said, "You may be impacted, and we've already started protecting you."

Why This Matters

This story shows the importance of Big R thinking and why it's essential to jump into action quickly without waiting for clear-cut alerts. Alerts can come from the most unexpected sources, such as a third-party notification instead of a system trigger. Thinking beyond the immediate threat and taking early action can prevent additional compromises.

In this case, the SOC managed to protect three other clients who had no idea they were at risk.

One IP Address, Two Organizations Saved

On the surface, it looked like the alert had been resolved, and the case could be closed. But one analyst's curiosity led to a deeper investigation, uncovering a hidden threat that could have gone unnoticed.

A Malicious IP That Wouldn't Go Away

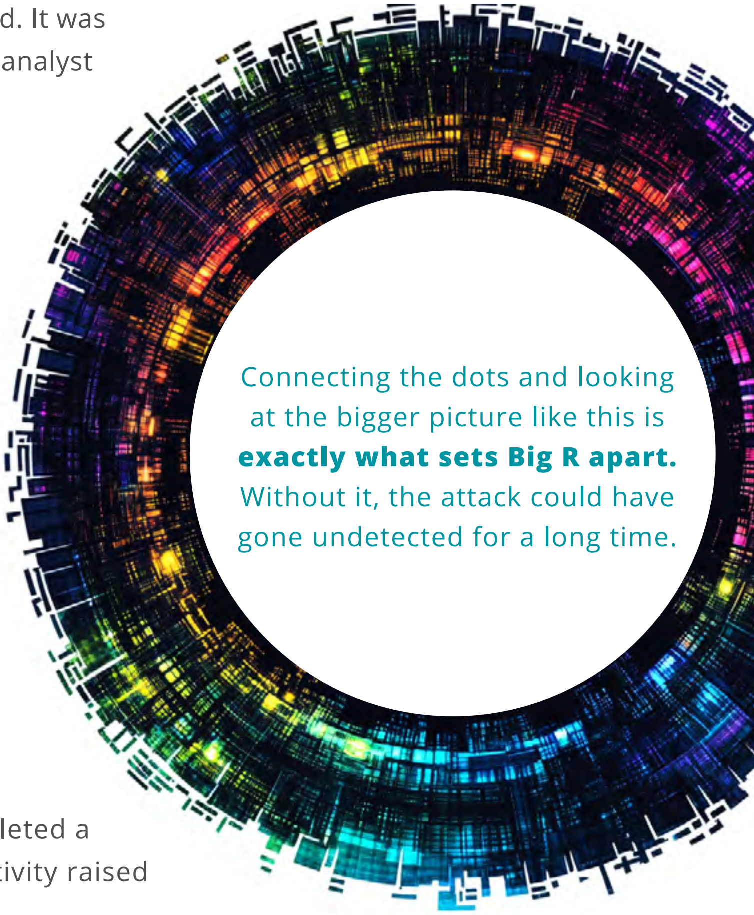
The initial alert was resolved, but one IP address repeatedly appeared. It was easy to brush it off, but one analyst wasn't ready to let it go.

They decided to search for that same IP across other client environments to see if there was more to the story.

The Hidden Sign-In Trail

When the analyst dug deeper, they found that the same malicious IP from the initial alert had been used to sign into Outlook Mobile for a second client.

So far, the user had just deleted a few PTO emails, but the activity raised red flags.



Connecting the dots and looking at the bigger picture like this is **exactly what sets Big R apart.** Without it, the attack could have gone undetected for a long time.

It hadn't triggered any alerts, and the behavior didn't initially seem suspicious, but the analyst realized there was more at play.

Preventing a Future Attack with Pattern Recognition

The pattern was clear: the same IP address was used across multiple clients, and the login behavior had anomalies, including email deletions, without any alerts.

By recognizing these patterns, the analyst could prevent a future attack and stop the compromise before it could escalate.

Why This Matters

Cross-client awareness and pattern matching across multiple accounts can help to prevent damage that others can't see.

A Malicious Inbox Rule and 300+ Shares

It started with the CyberMaxx team receiving a peculiar alert for “O365 - Known Malicious Inbox Rule.” But what initially seemed like a minor oddity quickly snowballed into a large-scale incident, triggering a rapid investigation and a major containment effort.

Small alerts often signal larger problems beneath the surface. Responding quickly helps protect your systems more effectively.

A Rule That Didn’t Belong

The alert came through as a “known malicious inbox rule” in O365. It automatically moved any email containing a “.” to a newly created folder. At first glance, it was highly suspicious, as these rules are often used to make malicious activity more difficult to spot.

Thanks to their extensive experience, CyberMaxx’s analysts immediately recognized the potential threat.

Logins and a Suspicious PDF

The first sign-ins from a known bad IP address began on March 7. A few days later, on March 12, “User1” uploaded a PDF to SharePoint. The creation of the suspicious inbox rule immediately followed this.

Individually, these activities look very minor. But together, they suggested something much deeper.

300+ Emails Sent

The threat escalated quickly, and the PDF uploaded to SharePoint was sent over 300 times to internal and external users.

To make things worse, “User2” had already clicked on the link, exposing more potential vulnerabilities. The scale of this attack shows how powerful automation can be when it comes to cyberattacks.

Containment and Further Discovery

CyberMaxx advised the client to disable the compromised account, revoke active sessions, and engage their Incident Response protocol while we investigated the issue further.

Our investigation showed that the attack had gone even further than expected and that eight additional accounts had been compromised, all linked to the same malicious IP.

Why This Matters

CyberMaxx’s full-scope evaluation meant the client could act quickly and contain the incident before it spiraled out of control. As a result, more users were protected from compromise.

From a Physical Threat to Cyber Defense

CyberMaxx analysts know that security risks can quickly cross boundaries from the digital world and into the physical world, so they monitor a wide range of sources. When a physical security issue triggered an investigation, it led to a deeper understanding of a potential cyber threat. It's proof that no lead is too small to investigate thoroughly.

The CHIME Alert That Triggered a Deeper Look

CyberMaxx received a physical security alert from The College of Health Information Management Executives (CHIME), a healthcare security group. While others might have just forwarded it and moved on, we dug deeper just in case.

The alert hinted at a possible cyber threat, and we knew it was important to pay attention — even when things didn't seem directly related at first.

A Thread Worth Pulling

CyberMaxx's threat intel team took the alert seriously. After looking more closely, we realized the incident could potentially trigger a cyber attack from sympathetic nation-state actors.

We could have waited for more signs of an attack, but we decided to get ahead by trying to connect the dots and explore potential angles.

Lots of providers would just send out the alert and stop there. **But Big R is all about proactive thinking.**

Preemptive Client Protection

We immediately notified relevant clients and ramped up our monitoring and protective measures to safeguard them against potential attacks.

That way, they were positioned to respond effectively if anything did happen.

Why This Matters

By investigating what others might overlook, CyberMaxx helped its clients uncover hidden threats before they could escalate.

A Thumb Drive and a Criminal Investigation

As threats become more complex, responding appropriately requires a delicate balance of ethical considerations, human judgment, and legal responsibility. In one case, what looked like a simple device turned out to be a sign of much more nefarious criminal activity.

Suspicious Files and Unusual Activity

Upon further inspection of the thumb drive, we quickly discovered that the tiny device was running its own programs and acting as a mini-computer. That behavior raised suspicions, prompting our analysts to take a closer look.

Confirming the Unthinkable

The files' contents revealed disturbing evidence involving illegal activity with minors. That escalated the incident from being just another breach to a full-blown criminal investigation.

We immediately paused our usual response protocols and implemented a different set of procedures.

Coordinating with Federal Authorities

Before contacting the authorities, we needed to confirm and verify the data. Once we contacted them, they guided us on how not to interrupt the activity but to monitor it.

The insight allowed them to make a greater impact. It clarified whether they were dealing with a lone actor or an organized group.

Ethical, Human-Led Escalation

CyberMaxx had to act quickly but carefully. We needed to make sure all of our actions were legal and ethical.Following the analysis, we notified the required channels in the organization and filled them in on what was happening.

This instance shows the limitations of AI. While it may be good at highlighting patterns and anomalies in data, i**t can't make important ethical decisions like humans can.**

Why This Matters

In situations like this, it's essential to understand when it's appropriate to take a step back and get others involved.

Why Big R Works: Human Judgment and Creative Thinking

While technical tools were essential when it came to solving these challenges, there's another common thread running through all of these stories: human insight drove every single successful outcome.

The SOC's creative, iterative approach to threat hunting shows the importance of critical thinking and challenging assumptions over sticking to rigid playbooks when solving complex security challenges.

The Boss Method: Don't Assume Anything

You might have heard of Bruce Springsteen's creative songwriting process. Whenever he gets stuck, he returns to the song and finds his favorite line. Then, he throws it out because it limits his creativity for the rest of the song. CyberMaxx analysts follow the same method: They toss out their favorite theories and start fresh when they hit a roadblock.

Letting the Data Tell the Story

Sometimes, letting an activity play out a little longer is essential to help build a clearer picture and understand the threat more thoroughly. Instead of rushing, we simply observe. We think like an adversary. We call this our "consequence of determination" approach.

Think Like an Adversary. Defend Like a Guardian

CyberMaxx's approach combines the most up-to-date technology with relentless human curiosity, judgment, and perseverance. Instead of scrambling to contain threats after they've already caused problems, we think adversaries should anticipate threats before they happen.

Then, we defend like guardians to ensure your security.

THINK LIKE AN ADVERSARY
DEFEND LIKE A GUARDIAN

Ready to take the first steps towards a stronger security posture? Schedule an introductory call with one of our solutions experts today.

For more information, call 1-800-897-CYBER (2923) or visit: CyberMaxx.com