MBA Research & Curriculum Center

Breaking Tech for the Better: Offensive Security for Threat Detection

As we learn from the business world, we want to share that information with our community of educators and business professionals. Recent focus panels, which serve as a space for business professionals to share insights, have highlighted the growing importance of what is commonly known as offensive security, or breaking down key processes or technology to identify risks and areas for growth. The following Action Brief offers an introduction to this fascinating side of process improvement and discusses prominent examples in the business world today.

From Russia With Love

The year is 2021. Kaseya Limited is a rising star in the world of information technology, cybersecurity, and network monitoring. The firm has just been valued at over $2 billion for the first time in its 21-year history.

But suddenly, Kaseya finds itself in the middle of a disaster straight out of a Hollywood spy thriller.

A Russian cybercrime syndicate called REvil (yes, they literally had "evil" in their name) has exploited several bugs in Kaseya's software to deploy a ransomware attack. Kaseya is forced to completely shut down its servers, but the damage has been done—thousands of Kaseya's customers are locked by ransomware. The cybercriminals demand millions in ransom payments from each client affected, as well as a staggering $70 million from Kaseya itself.

The problem is so widespread that the Commander in Chief has to get involved! One week after the ransomware infiltration, President Biden confronts Russian President Vladimir Putin about the cyberattack and demands that he take action against those responsible.

A few weeks later, all ransomware is finally unlocked by the FBI, and the hacker group REvil vanishes from the internet. And while Kaseya never had to pay the $70 million, experts estimate the total financial and reputational consequences of the attack to be in the hundreds of millions.

Red Team, Deploy!

The year is 2025. Kaseya's annual revenue has more than doubled since 2021, its product offerings and client base have greatly expanded, and its valuation now exceeds $12 billion. The company even owns the naming rights to the Miami Heat's arena!

So how is it that such a catastrophic cyberattack just a few years ago didn't cripple Kaseya's growth? How did the company recover?

Kaseya completely overhauled its cybersecurity systems. Most notably, it embraced a rising trend that was also highlighted by business leaders at a recent MBA Research focus panel: hiring employees specifically to stress-test—or "break"—its own processes.

Employees who perform this task are typically called "red teams." Red teams are responsible for testing the effectiveness of their company's various systems or technologies to detect any threats or vulnerabilities.

The interconnectedness of the modern business world has made the role of red teams essential. Companies today are increasingly reliant on numerous services and products available through global digital infrastructure (third-party software packages, cloud computing, data centers, etc.). Therefore, many companies need professionals who are fully devoted to threat identification to prevent risks that cascade from (or to) other organizations.

Offense Is the Best Defense

Just a few months after resolving the ransomware attack on their software, Kaseya actually hired one of the FBI agents who helped it recover from the attack. Among many other cybersecurity overhauls, the former FBI agent created red teams to thoroughly interrogate all of Kaseya's cyber infrastructure.

And Kaseya isn't the only big company to improve its processes through an "offensive security" posture:

- Meta's "Red Team X" features a roster of both hardware and software "hackers" responsible for vetting their company's digital capabilities. In the past, the team has created fake bots, conducted cryptojacking simulations, and even used portable network routers to trick Meta employees into joining fake Wi-Fi networks at Meta's headquarters in Menlo Park, California. ("1 Hacker Way" is the address for Meta's campus, funnily enough.)
- IBM's "X-Force Red" conducts extensive testing on third-party hardware that runs on IBM technology, including key products like medical devices, automotive computers, and ATMs. IBM even has several facilities worldwide that operate exclusively as testing facilities for their red teams.
- Google's red team has been allowed maximal creativity in how they can test the resilience of the cybersecurity measures. This allows the red team to use real tactics a hacker might employ to break into Google's network. Once, the red team literally sent USB plug-in toys to Google employees as work anniversary gifts. The twist was that the toys were malware-enabled, allowing the red team access to the computer of any employee who plugged in the toy!

In addition to the tech industry, the finance sector has also experienced a growth in red teaming. Professionals from a recent finance focus panel explained how many firms today are hiring dozens of engineers with a focus on breaking down technology. Some even mentioned the strategy of competitive red teaming, where engineers will break down a competitor's technology to better assess what makes it special and build a better product in its place.

Breaking Chatbots

The explosion in artificial intelligence (AI) capabilities has given red teams a new project: Refining AI (particularly generative AI) by discovering errors, hallucinations, and threats.

We've all seen stories of (or experienced) chatbots giving incorrect, offensive, or even illegal advice to users. And as long as regulations around AI remain sparse, tech giants are employing their red teams to help them self-regulate the outputs of AI:

- OpenAI, creator of ChatGPT, uses red teaming to prevent dangerous AI outputs by detecting vulnerabilities and inconsistencies in the AI model.
- Chipmaker NVIDIA conducts two types of red teaming: *content* (monitoring potentially compromising prompts and outputs) and *cybersecurity* (detecting security risks within the technology stack powering the AI program).
- Microsoft's AI Red Team performs extensive testing to ensure that AI models follow safety instructions, keep sensitive training data secure, and remain resilient in the face of external attacks.

The true value proposition of AI in business remains hotly disputed, but one thing's for sure: Red teams will remain an effective security blanket for AI, whatever the form AI assumes in society. While ethical dilemmas, controversies, and even whispers of a dreaded "AI bubble" persist, we can take some comfort in the fact that most AI infrastructure already has proactive security systems in place. Because, as the role of AI in business continues to grow, the need for robust red teams and rigorous offensive security measures will only increase.

Links for Further Reading:

- "Meet the Hackers Who Are Trying to Make AI Go Rogue"
- "Can We Red Team Our Way to AI Accountability?"
- *Red Team | Hacking Google | Documentary EP003*

Discussion Questions:

- One of the main reasons Kaseya could be hacked was that the company had ignored bugs and glitches in its system. How could a red team have helped the company avoid succumbing to a cyberattack in the first place?
- How might having a red team—or simply a "red team mentality"—help prevent groupthink within an organization?
- Besides cybersecurity and AI, can you think of any business sectors that might benefit from deploying red teams?
- Can you think of any other creative ways a red team could test or simulate the security of their company?
- Do you think it's especially important to have red teams for chatbots and other generative AI? Why or why not?

Sources:

- "11 Famous AI Disasters"
- "Advancing Red Teaming With People and AI"
- "AI Valuation Fears Grip Global Investors as Tech Bubble Concerns Grow"
- "Defining LLM Red Teaming"
- "Experts Worry AI Is Driving Layoffs, Even as It's Not Really Delivering on Its Promises"
- "Former FBI Agent Thought He Had Seen It All in Cybercrime. Then He Became a Corporate Executive in Charge of Information Security"
- "Google's Hackers: Inside the Cybersecurity Red Team That Keeps Google Safe"
- "How Google Does It: Red Teaming at Scale"
- "How OpenAI Stress-Tests Its Large Language Models"
- "IBM Security Opens Network of Four Secure Testing Facilities Globally"
- "Meta Takes Offensive Posture With Privacy Red Team"
- "Microsoft AI Red Team: What Is It, and Why Is It Critical for Security?"
- "NVIDIA AI Red Team: An Introduction"
- "Red Teaming Landscape & Why Red Teaming Is Crucial For Businesses"
- "What Is a Red Team Exercise & Why Should You Conduct One?"
- "What Is ChatGPT, DALL-E, and Generative AI?"
- "What Is Offensive Security and Why Is It So Challenging?"
- "What Is Ransomware?"
- "What Is Red Teaming?"
- "What Was the Kaseya Ransomware Incident About? Who Was Affected and What Was the Cost to Everyone?"
- "Will AI Save Or Harm Us? 3 Ethical Challenges for Businesses In 2025"
- "X-Force Red Offensive Security Services"
- "What Is Cryptojacking?"