Enterprise Strategy Group by TechTarget

SHOWCASE

JUNE 2023

Active Defense and Deception Technology: The Time is Now!

Jon Oltsik, Distinguished Analyst and Fellow

Abstract: Security operations requirements, like threat detection and response, continue to grow more challenging each year. According an Economic Validation report from TechTarget's Enterprise Strategy Group, it can take 168 hours or more, on average, to identify threats, while many threats are never detected.[1] Therefore, CISOs should consider deception technology for improving threat detection and response. Modern deception technology like FortiDeceptor combines the historical value of deception technology with ease of use, automation, and actionable intelligence—creating an active defense. These benefits are especially important for organizations with limited security staff and skills and those merging IT and OT.

Threat Detection and Response Is Increasingly Challenging

According to research from Enterprise Strategy Group, more than half (52%) of organizations say that security operations, like threat detection and response, are more difficult today than they were two years ago because (see Figure 1):[2]

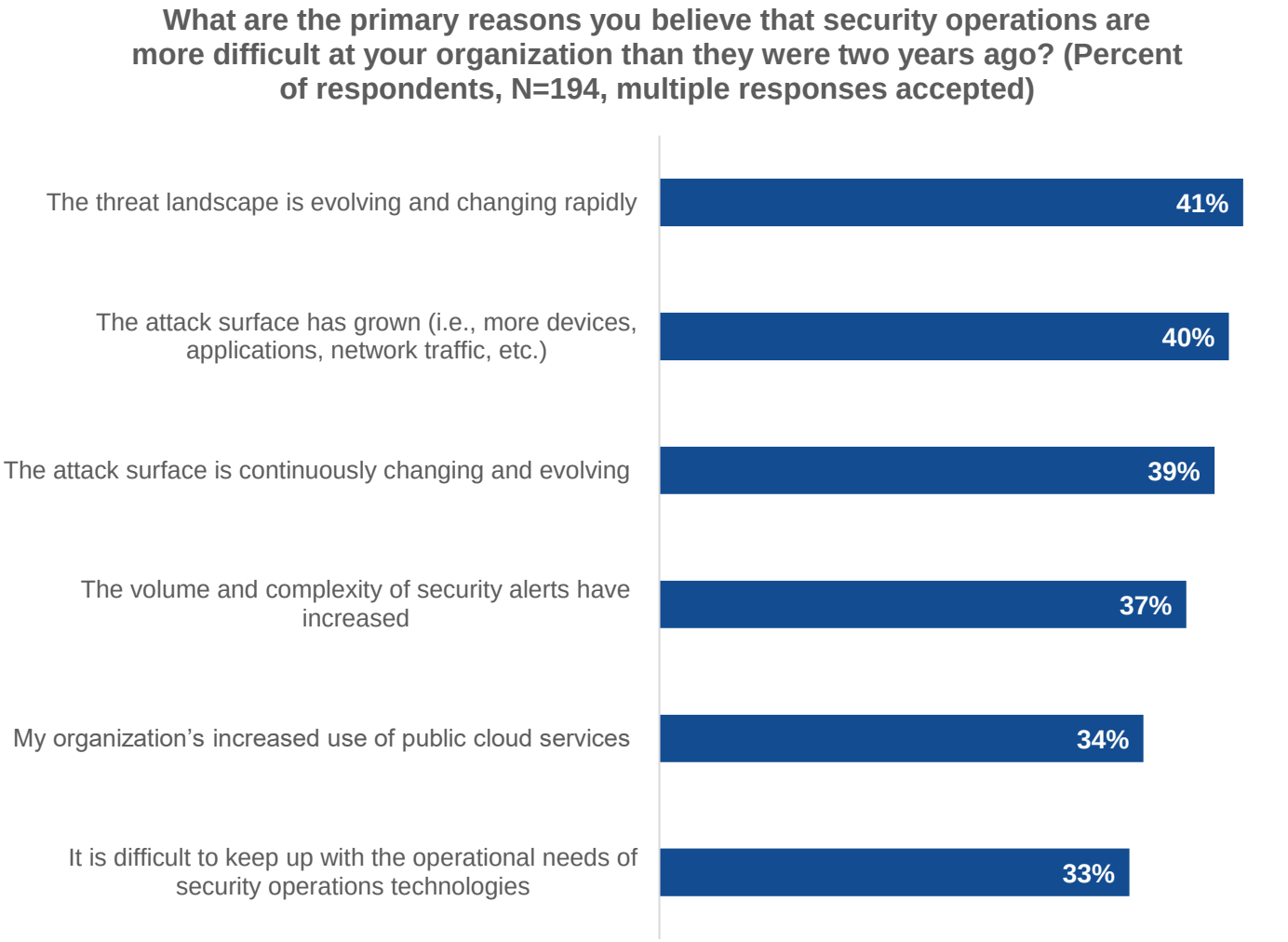
- **The threat landscape is evolving and changing rapidly.** Cyber-adversaries cooperate and specialize, using attack tools previously limited to state actors. Many attacks also use automated tools for tactics like scanning the attack surface looking for vulnerabilities, while others take advantage of available resources like utilizing generative AI systems like ChatGPT to create realistic phishing emails. Meanwhile, security teams struggle to keep up.
- **A growing attack surface makes defense a challenge.** In separate Enterprise Strategy Group research, more than two-thirds of organizations claimed their attack surface had grown over the past two years, driven by third-party connections, remote worker support, and digital transformation.[3] It is also noteworthy that 34% say security operations are more difficult due to the growing use of public cloud services—adding a force multiplier to attack-surface growth. Security teams must discover the attack surface, scan it for vulnerabilities, understand attack paths, and mitigate critical risks, all of which are easier said than done.
- **Alert volume and complexity overwhelm security operations teams.** Many organizations have dozens of threat detection tools, each of which produces a constant stream of security alerts. The security operations center (SOC) team must examine, prioritize, and triage these disparate alerts in real time. Some alerts are false positives, sidetracking the SOC team down time-consuming dead ends. Smaller enterprise organizations often staff their SOC with one or a few staff members, so alert storms can quickly overpower their ability to find true needles in the haystack.
- **Organizations can't keep up with the operational needs of their security technologies.** The growing portfolio of security tools adds to operational complexity, as each security technology demands constant care and feeding (i.e., customization, tuning, and so on). These activities require time and skills that are not always available, which could lead to misconfigured and ineffective security controls and related cyber-risks.

[1] Source: Enterprise Strategy Group Economic Validation, *The Quantified Benefits of the Fortinet Automated SOC*, June 2023.
[2] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.
[3] Source: Enterprise Strategy Group Research Report, *Security Hygiene and Posture Management*, January 2022.

Security operations challenges are especially pronounced in industries like healthcare, manufacturing, and critical infrastructure, where security teams are responsible for threat prevention, detection, and response for IT and OT. These firms are often understaffed and lack some advanced security skills. A breach could disrupt operations, like halting a manufacturing line, or impact the delivery of critical services like electricity, water, gas, or healthcare.

Organizations like these have also been quite susceptible to ransomware attacks, due to monitoring gaps, controls deficiencies, or a lack of detection engineering management.

Figure 1. Top 6 Reasons Why Security Operations Are Growing More Difficult



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Case for an Active Defense Using Deception Technology

CISOs can't be satisfied with status quo security when detecting and responding to sophisticated attacks is increasingly difficult and the balance of power is tipping toward adversaries. What's needed? An active defense that fully utilizes the power of deception technology. Used properly, deception technology can:

- **Create a realistic parallel universe across hybrid IT**. Deception technology can create decoys (fake systems), lures (fake services), network traffic (fake packets and protocols), and breadcrumbs to attract adversaries, and persuade them to go after the deception assets rather than the real ones. In this way,

deception technology can create a "home-field advantage." For example, by creating a deception network 10 times larger than their real network, cyber-attacks become more costly and difficult for adversaries. For defenders, deception can lead to early detection and neutralization of cyber-attacks.

- **Produce only high-fidelity alerts.** Deception assets are invisible to legitimate users, meaning that when they are accessed, there must be some type of malicious activity going on. For example, deception technology can detect lateral movement by placing fake credentials, files, and applications on endpoints. When an attacker steals these fake credentials from endpoints to move laterally, deception will instantly detect this malicious pattern. Overall, deception technology provides accurate and timely alerts, greatly reducing security operations complexity while accelerating mean time to detect (MTTD) and mean time to respond (MTTR) to real security events.
- **Drive the creation of real-time blocking rules.** Deception technology can improve detection and the efficacy of security tools, such as network access controls (NAC), endpoint detection and response (EDR), and network detection and response (NDR), providing early detection of an attack even before the attacker engages with any real asset in the network. Deception technology can also be integrated with firewalls, network proxies, and intrusion prevention systems. When detection platforms detect an intruder, they can generate blocking rules for security controls (i.e., blocking IP addresses, network ports, web domains, files, and so on).
- **Help organizations with merged IT and OT environments.** Deception technology can create decoy OT/IoT assets and emulate OT/IoT network traffic to entice adversaries. Once threat actors access a deception asset, security teams know they are under attack. They can then take immediate actions like blocking IP addresses, quarantining systems, and conducting more thorough forensic investigations.
- **Detect and prevent the spread of ransomware attacks by redirecting malware or ransomware from production systems to decoys**. By placing fake, shared file systems and files on endpoints, ransomware that targets files/shares is immediately detected and quarantined once it engages with fake assets.

FortiDeceptor Can Enable an Active Defense

Deception technology can be effective, but many security professionals still think of it as a complex science project for elite organizations. In truth, innovative deception technology enhances honeypot/honeynet systems with intelligence and automation, taking away many of the historical limitations. For example, FortiDeceptor is a modern, dynamic, automated deception platform that provides a defense layer across an entire hybrid IT infrastructure. FortiDeceptor, available as a software-as-a-service offering, VM, or hardware appliance, marries traditional deception technology with high-priority enterprise requirements with:

- **Easy setup and time to value.** FortiDeceptor actively or passively discovers network assets and segments. Based on these discoveries, the platform suggests a series of deception decoys (i.e., decoys run from the FortiDeceptor appliance using the available/unused IP addresses. FortiDeceptor makes it seem like these decoys run from an organization's network segments.) placed in strategic locations across the network, those most likely of interest to cyber-adversaries, in addition to tokens that are placed on real endpoints and servers, providing complete coverage. FortiDeceptor is agentless and requires no changes to the network topology, easing the setup phase. To keep up with the changing threat landscape and attack surface, FortiDeceptor can be customized and updated automatically as the environment changes.
- **Accurate and timely detection alerts**. Since fake assets can only be accessed for nefarious purposes, FortiDeceptor alerts are, by definition, accurate and actionable, avoiding false positives. FortiDeceptor also correlates alerts to known malicious activity, helping analysts investigate, gather forensic evidence, monitor, and automatically respond to attacks in progress. Attacks can be replayed to help blue teams assess defenses, discover gaps, and then bolster existing security controls. Since FortiDeceptor can track adversary movement, security analysts can also use its output to enhance activities like threat hunting and research.
- **Integration with the Fortinet security fabric.** FortiDeceptor can be integrated with other security tools, such as firewalls, NAC, EDR, malware sandbox, NDR, SIEM, and SOAR tools; it is also part of the Fortinet Security Fabric, providing orchestrated attack isolation, advance threat detection, and enriched threat analysis.

FortiDeceptor is especially useful for organizations with merged or merging IT and OT environments. It can create lifelike decoys of many OT technologies, like PLC and SCADA management systems and can emulate their traffic patterns and protocols, as well as those of many IoT technologies like network switches, printers, IP cameras, and medical devices. Fake but realistic IoT/OT devices across the network tend to confuse adversaries, forcing them into mistakes that are then captured as high-fidelity alerts. To further enhance its IT/OT coverage, FortiDeceptor supports the MITRE Engage and MITRE ICS frameworks, mapping forensics details, and classifies alerts based on the framework. Analysts can filter the alerts by multiple MITRE tactics and techniques for streamlined analysis.

FortiDeceptor maintains authentic and up-to-date deception layers that can be scaled as the threat level increases, with relatively little effort. This is achieved, for example, by automatically deploying decoys with recently disclosed vulnerabilities to attract, detect, and quarantine malicious activities early in the kill chain. In addition, FortiDeceptor can automatically refresh deception assets and deploy new ones based on suspicious activities, network topology changes, attack surface growth, and the like. This makes FortiDeceptor, with its accurate early detection and automated response, a strong defense for attacks including ransomware.

Conclusion

Detecting and responding to threats in a timely and accurate manner is demanding and becoming even more difficult. While many technologies promise better results, they still require overhead, generate false positives, and must be integrated into numerous other security systems. Unfortunately, many organizations simply can't keep up.

Deception technology is well established but often misunderstood. Some organizations believe that deception technology remains the domain of advanced security teams, but this is a fallacy. Innovative deception technology, like FortiDeceptor from Fortinet, combines the value of honeypots and honeynets with ease of use, automation, actionable intelligence, and integration with existing security controls, creating an active defense. These benefits are especially important for organizations with limited security staff and skills and those merging IT and OT.

CISOs at organizations like these may want to explore how deception technology like FortiDeceptor can help them accelerate MTTD and MTTR while streamlining security operations. As one user told Enterprise Strategy Group, **"FortiDeceptor is a huge value for us, as it puts out honeypots to detect attempts to login with disabled credentials or from suspicious locations and blocks potentially malicious IPs before they do damage."**

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com