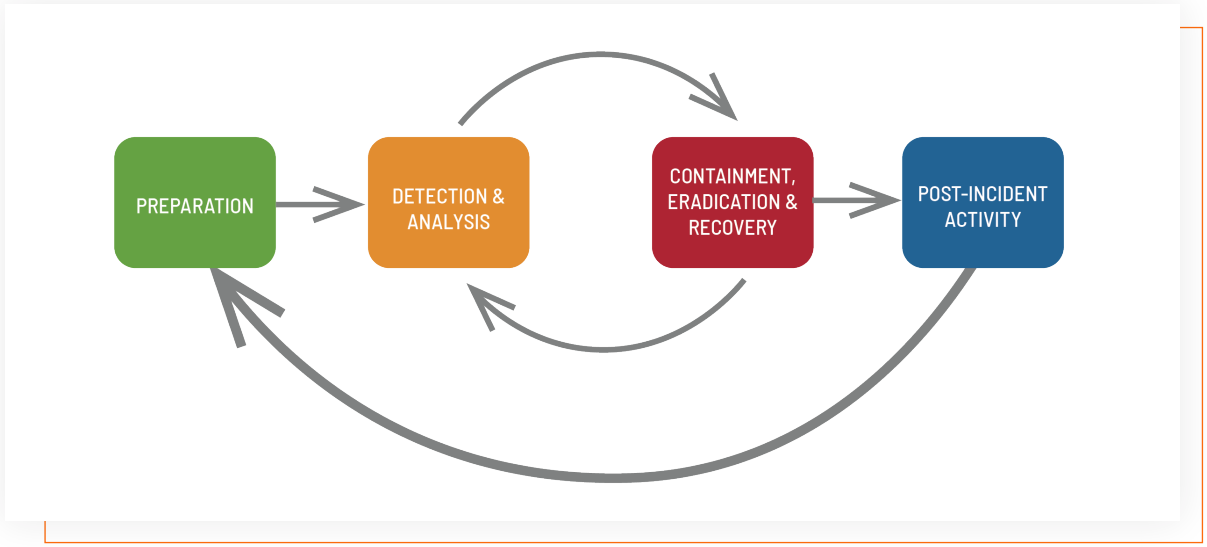
THREATDEFEND® DECEPTION PLATFORM FOR AUTOMATED INCIDENT RESPONSE

As the number and complexity of threats facing security professionals increases, incident response capabilities are as critical as ever. The challenges in conducting a flawless incident response plan, however, are equally as complex as the threats they try to remediate. As an incident response may be cumbersome, automating the steps involved not only reduces time-to-remediation, but it also unburdens critical resources from alert fatigue, necessary actions in successfully avoiding a breach.

New technology plays a critical role in solving these challenges and providing continuous threat management for early detection and automation of incident handling for faster remediation. One of these is the Attivo Networks® ThreatDefend® platform's ThreatOps function, which can create repeatable playbooks to automate incident response investigations and actions for consistent and accelerated performance..

INCIDENT RESPONSE ISSUES

Incident response (IR) is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to address the event to limit the damage, manage liability, and reduce recovery time and costs. To this end, many organizations have dedicated personnel, the Computer Security Incident Response Team (CSIRT), to manage and be responsible for the IR process.



Incident Response Life Cycle

Current methodologies detect incidents by placing different solutions throughout the network to collect data while protecting network perimeters and endpoints. These solutions gather communications and activity data, which a security monitoring function analyzes to identify incidents. The analysis of this data can be integrated within the solution (such as firewalls, intrusion detection/prevention systems, or antivirus at the endpoints), automated with Security Information and Event Management (SIEM) software, or conducted manually by security personnel. Identified malicious activity raises alerts for the CSIRT to investigate and confirm the incident. Discovering a security event begins the IR process, with the CSIRT conducting all necessary steps to contain and remediate the threat. Early detection is essential to preventing a breach, but attackers have ways to not only evade detection but also dwell for extended periods inside the network.

Many factors allow attackers to evade detection. They include;

- Imperfect detection: Attackers can alter attack patterns and binary hashes to evade signature-based detection. Anomaly detection can generate false positives or false negatives that attackers take advantage of to slip through.

- Signal-to-noise ratio: High volumes of data and alerts make data correlation difficult, leading to high noise, missed incidents, and false positives to sift through.

- Resource constraints: Security organizations are severely resource-limited, particularly in recruiting, training, and retaining talented security professionals. The lack of experienced security personnel and the increasing numbers of open security positions make this a problem that will persist for some time.

SECURITY OPERATIONS ISSUES

Security Operations (SecOps) are the operational activities related to the people, processes, and technologies involved in providing situational awareness through the detection, containment, and remediation of IT threats. Security Operations are functions of the Security Operations Center (SOC), and are usually centered around a SIEM solution, as well as aggregating and correlating data from security feeds. These include network discovery, vulnerability assessment, Governance Risk and Compliance (GRC) systems, website assessment and monitoring, application and database scanners, penetration testing tools, IDS/ IPS devices, log management systems, network behavior analysis and cyber threat intelligence, wireless intrusion prevention system, firewalls, antivirus, and unified threat management (UTM). The SIEM functions as a central consolidation point or "single pane of glass" for the security analysts to monitor the security information. SecOps teams usually include security analysts, security engineers, security managers, and the CSIRT, and all share the shared tasks of keeping the organization secured.

IR AND SECOPS CHALLENGES

IR and SecOps consistently cite the following issues as challenges to security, and although there are many products on the market that try to address them, they remain unresolved.

- Detection issues, particularly with false negatives and false positives
- Extremely high volume of alerts leading to increased workload, false positives, and alert fatigue
- Faster compromises, longer detection times
- Insufficient skilled personnel to fill vacancies, and difficulty retaining experienced personnel
- User carelessness and lack of security awareness
- Visibility gaps in networks of growing complexity
- Higher volumes of malware and attacks that bypass detection mechanisms
- Inability to coordinate efforts between departments
- Patch/vulnerability management issues, and dependence on legacy applications

These challenges impact an organization's ability to investigate and respond to incidents effectively. Many organizations are adopting deception-based detection solutions with automated attack analysis and incident response to address these challenges efficiently.

THE THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend platform is an effective and efficient detection solution that reveals in-network attackers early, accurately, and a response platform for automating investigations and incident response. It includes the Attivo BOTsink® deception servers, which support the creation and management of decoys, Informer dashboard for adversary intelligence viewing, and ThreatOps® incident response orchestration playbooks. The virtual environment can also function as a sandbox for malicious binary and suspicious e-mail analysis. The portfolio also includes the Endpoint Detection Net suite, composed of the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, and the EDN manager. For scalable deployment, organizations can also add ThreatDirect deception forwarders to support remote and segmented networks and the Attivo Central Manager (ACM) for enterprise-wide deception fabric management.

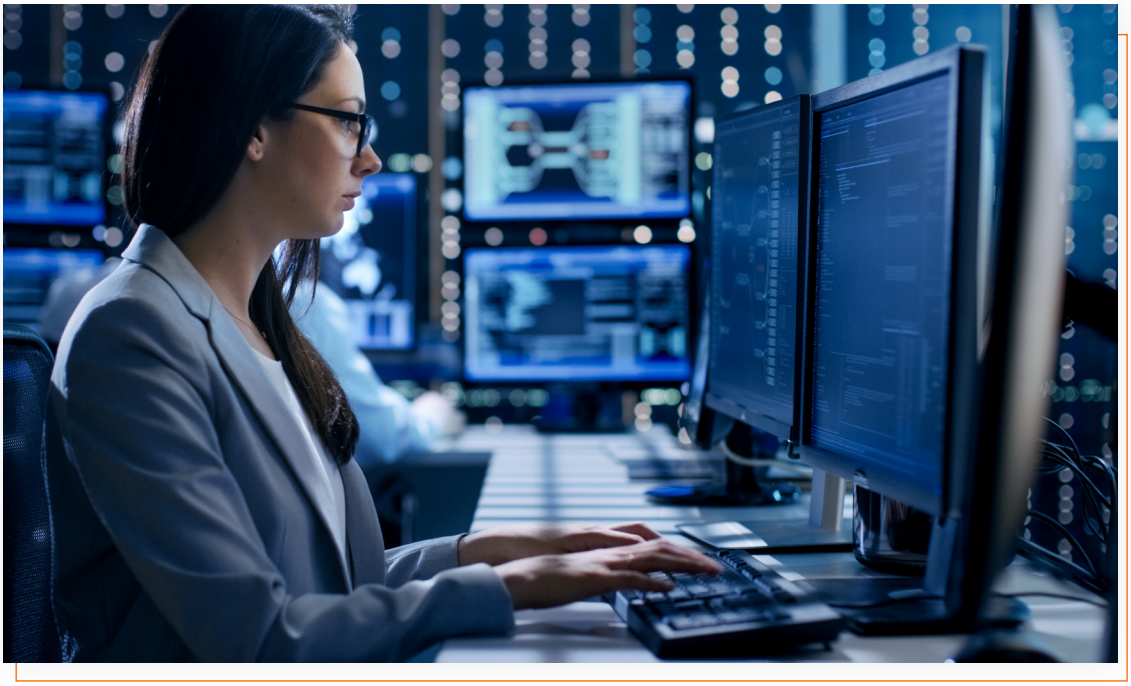
> After we deployed the ThreatDefend Platform, we saw our mean time to respond to security incidents go from four hours down to fifteen minutes.
>
> - Director of Cybersecurity, State University

DEALING WITH INCIDENT RESPONSE CHALLENGES

The ThreatDefend platform addresses IR issues in several ways. First, the platform only alerts on confirmed attacker activities. The engagement servers acting as decoys invite attacker attention. When an attacker compromises a decoy system, the platform generates an alert while responding to the attacker. As the attacker engages with the engagement servers, the system captures forensic data and correlates the events. The platform only alerts on confirmed attacker activity and does not depend on signatures or behavioral analysis, minimizing false positives and eliminating false negatives.

Furthermore, the platform substantiates the alerts with evidence-based analysis. The engagement servers record all activity occurring in the decoy environment, including network activity, memory space, and virtual storage, collectively minimizing the risk of false positives. The volume of alerts from the platform is minimal, reducing the chance of alert fatigue, which directly addresses the problem of a low signal-to-noise ratio and will not "light up like a Christmas tree," unless an attacker has already compromised the organization.

Since the alerts happen when the attacker engages with the decoys, whether through reconnaissance or from following a deceptive lure stolen from the endpoints, there is no delay in detection times. The alert happens in near-real-time, reducing detection delays and enabling the CSIRT to begin the incident response process immediately. CSIRT personnel increase response efficiency substantially with the reduction in alert volume, as well as time-saving third-party integrations and automation.



MITIGATING SECURITY OPERATIONS CHALLENGES

With the ThreatDefend platform in the environment, organizations can mitigate their SecOps issues for which there is no immediate solution. With the built-in sandbox analysis capabilities, users can send suspicious e-mails to the CSIRT, utilizing the ThreatDefend Platform to analyze them automatically and produce detailed reports of malicious activity. Even if a user accidentally opens a malicious e-mail, the platform's advanced detection capabilities are on the alert to detect when the attacker attempts to move laterally to other victims or servers on the network.

With deployment flexibility, organizations gain visibility throughout the environment and simplify overall threat monitoring on-premises, in the cloud, at remote sites, or in specialized network segments. Even with attacks that evade detection, once an attacker enters the network and conducts reconnaissance or moves laterally, the ThreatDefend platform will detect them. Increased visibility alleviates the concerns of unpatched, vulnerable, or legacy systems, and the platform can identify exposed credentials, which are often not found with other vulnerability assessment tools. Even if an attacker makes use of a zero-day vulnerability to attack an unpatched legacy system and compromise an endpoint, any attempt at reconnaissance or lateral movement generates alerts that an adversary is in the network. Additionally, through integrations with SIEM vendors, the platform can query logs to find failed logins based on the attempted use of deception credentials.

These features make the Attivo ThreatDefend Deception and Response Platform an ideal solution to meet the IR and SecOps challenges of any organization.

THREATOPS ORCHESTRATION PLAYBOOKS

To decrease the workload on CSIRTS, organizations utilize automation and orchestration to ensure that security teams execute all appropriate actions in the response playbooks. The ThreatDefend Platform's ThreatOps playbooks enable this orchestration through numerous third-party integrations that automate attack data correlation and incident response activities. These integrations include SIEMs, firewalls, NAC solutions, endpoint isolation, and even enterprise search for threat hunting, extending the value of existing solutions already in the environment. The platform automatically correlates attack data and can create playbooks and for rapid response and adherence to security policies. Additionally, automation capabilities, coupled with built-in collaboration functions, make these processes repeatable and ease coordination with other departments, while establishing historical records and playbooks to enhance training. The ThreatOps playbook's capabilities enable a CSIRT to automatically and immediately execute response actions, such as adding firewall/IPS rules or quarantining infected endpoints to prevent the spread of ransomware, saving valuable time and resources. Additionally, the platform integrates with party endpoint providers such as Carbon Black, ForeScout, and McAfee EPO for threat hunting and threat intelligence exchange to look for other forensic artifacts or infections throughout the network. These capabilities close the loop on whether the security teams have truly eradicated the threat from the network.

CONCLUSION: WRAPPING IT UP

There are many challenges faced by IR and SecOps that technology innovations can now address. The Attivo Networks ThreatDefend Platform accurately and efficiently addresses these challenges while extending the value of existing security infrastructure. The ThreatOps orchestration playbooks take advantage of the platform's native integrations with existing partner security solutions to automate and accelerate incident response and intelligence sharing. Organizations seeking to simplify and improve their security will realize significant benefits in deploying the ThreatDefend platform.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 130+ awards for its technology innovation and leadership.
Learn more: www.attivonetworks.com