WHITEPAPER

Attivo NETWORKS®

ATTIVO NETWORKS® THREATDEFEND® PLATFORM SIEM INTEGRATIONS

TABLE OF CONTENT

HIGHLIGHTS

The DevOps services allow teams to collaborate, develop code, build, and deploy applications. The following are some of the commonly used DevOps services in an organization.

- Real-time Threat Detection
- Attack Forensics, visibility and enrichment
- Threat Analysis and Automated Incident Response

OUTLINE

The rapid pace of attacks, existing security challenges such as staff shortages, and the ever-increasing alert volume drive the security industry to embrace the notion of consolidating data resources and orchestrating actions across vendors, open-source projects, and internal development efforts. Sharing information and codifying procedures makes the enterprise better equipped to ward off advanced threats with higher speed and greater accuracy.

ABOUT THE ATTIVO NETWORKS® THREATDEFEND® PLATFORM

Attivo Networks provides the ThreatDefend Detection and Response platform, a comprehensive solution that uses deception technology. The platform in real-time detects inside-the-network intrusions in networks, public and private data centers, and specialized environments such as Industrial Control System (ICS) SCADA, Internet of Things (IoT), and Point of Sale (POS) environments. Founded on the premise that even the best security systems cannot prevent all attacks, the platform provides the required visibility and actionable, substantiated alerts to detect, isolate, and defend against cyber attacks. Unlike traditional security controls that focus on prevention, Attivo assumes that the attacker is inside the network and uses high-interaction decoys and endpoint, server, and application deception lures placed ubiquitously across the network to deceive threat actors into revealing themselves. With no dependencies on signatures or attack pattern matching, the BOTsink® deception server accurately and efficiently detects the reconnaissance and lateral movement of advanced threats, stolen credential, ransomware, man-in-the-middle, and phishing attacks. The Attivo Multi-Correlation Detection Engine (MCDE) captures and analyzes attacker IPs, methods, and actions that the platform. It can then displays this data in the Attivo Threat Intelligence Dashboard; export it for forensic reporting in IOC, PCAP, STIX, CSV formats, or automatically updates SIEM and prevention systems for blocking, isolation, and threat hunting. The ThreatOps® function simplifies incident response through information sharing, incident response automation, and the creation of repeatable playbooks.

DETECTION

Deception technology provides better detection against attackers early in the attack cycle. Existing cybersecurity technologies struggle with the onslaught of sophisticated and persistent machine-assisted humans. These defense-in-depth technologies have a perimeter centric approach, and attackers have been able to consistently penetrate these networks, and move laterally within the organization unimpeded, eventually causing loss. Attacks have accelerated, and there is evidence that cyber attackers are penetrating traditional defenses at a rapidly increasing rate.

WHY INTEGRATE?

There are definite advantages to leveraging the detection capabilities that Attivo offers, sharing threat data, enriching it with contextual information, and organizing it to determine an appropriate response. Integrated threat intelligence helps security teams analyze data more swiftly and accurately.

Attivo Networks supports detection across the complete Security Incident Detection and Response kill chain:

- Collection: receives events using various protocols and sensors
  - Attivo Networks Value: Collect data at the endpoint, in the network and when an attacker engages
- Parsing: breaks down events and enters them into fields
  - Attivo Networks Value: Event information categorized into a queryable format
- Enrichment: adds contextual information to events
  - Attivo Networks Value: Look-up external threat intel databases for enrichment
- Indexing: stores events in the database
  - Attivo Networks Value: Event information forwarded to multiple factors
- Correlation: analyses and connects similar events
  - Attivo Networks Value: Events and sub-events categorized by attacker sessions
- Validation: checks event details across numerous sources
  - Attivo Networks Value: Minimal false positives because any engagement with a decoy is suspicious
- Response: takes action to counter a threat
  - Attivo Networks Value: Automated action taken based on configured parameters

DETECTION AND VISIBILITY CAPABILITIES

Attivo Networks offers visibility and detection of the following activities, including but not limited to:

- Deception threat events
- Deceptive credential usage
- Decoy engagement
- Data exfiltration
- Network discovery
- Man-in-the-Middle activities
- Attacker lateral movement
- Active Directory attacks or reconnaissance attempts
- Credential vulnerability and attack surface data
- In-depth process and query level visibility

With the above use cases, the platform sends high-fidelity alerts that include indicators of compromise (IoC).

Deception offers best-of-breed detection capabilities because the breadcrumbs, deceptive Active Directory responses, and real-operating systems create a decoy environment that attackers find nearly impossible to discern from a real one.

It is possible to send the high-fidelity, enriched, and indexed alerts to external SIEMs, which can then correlate the data across other deployed security solutions. Attivo Networks also provides repeatable incident response playbooks with native third-party integrations to automatically or manually block, quarantine, and hunt for threats from a deception-based detection. These actions include:

- Automatically project decoys in a suspicious network segment
- Running endpoint memory forensics
    - Collects memory forensic data about attackers and endpoints
- Quarantining a suspicious machine from the network
    - Automatically or manually isolates malicious IPs and hosts
- Inserting block rules to a firewall
    - Automatically or manually blocks with internal or perimeter firewalls.
- Correlate threat intelligence from other sources like McAfee TIE, VirusTotal, Reversing Labs, and others
- Execute a suspicious binary in a sandbox

HOW DOES IT WORK?

The Attivo Networks ThreatDefend Platform creates deceptive credentials with the Endpoint Detection Net (EDN) Suite and inserts them onto endpoints across the organization. Attackers can then steal and use the fake credentials across any of the organization's assets, whether on-premises like Active Directory, Exchange, or databases, or in the cloud such as Salesforce.com, Box.com, or Office365.com. The EDN suite also supports refreshing these credentials when deploying the application in service mode. When attackers steal these deceptive traces and attempt to log on to production servers, because they contain decoy account information, the attacker's login attempt fails. However, the SIEM agent or plugin installed on the production servers logs this failed attempt. Attivo Networks also recommends the organization monitor employees who are no longer with it.

Attivo Networks offers the widest variety of real and emulated decoys that can deploy across the organization. These can even project into the remote networks for greater efficacy. Additionally, the ThreatDefend Platform can also act as a malware analysis sandbox to analyze malware from a submissions email address it monitors and presents a report of the malware TTPs.

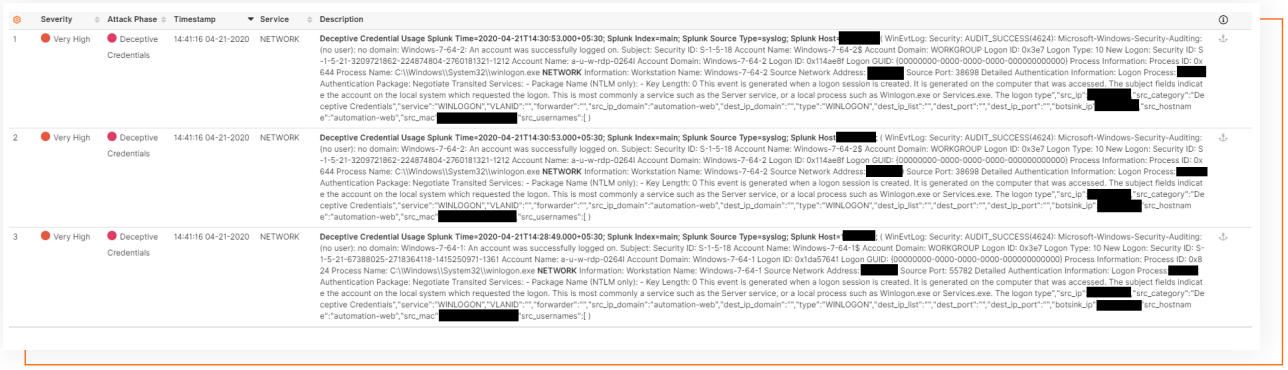
FORWARDING AND QUERY

The ThreatDefend platform can detect the most sophisticated threats, stop attackers, and empower the security team by giving them deep insights into the attacker's TTPs. The platform can reveal attacks early in the attack cycle by detecting activities from the initial access to lateral movement attempts. The ThreatDefend platform does this by forwarding information into the SIEM and also by querying it for stolen credential login failures. The ThreatDefend platform presents the attacker with a deceptive credential and detects the stolen credential's failure on a production system by querying for the SIEM logs. The platform then shows a correlated timeline view to these sporadic events giving insights into the attackers TTPs.

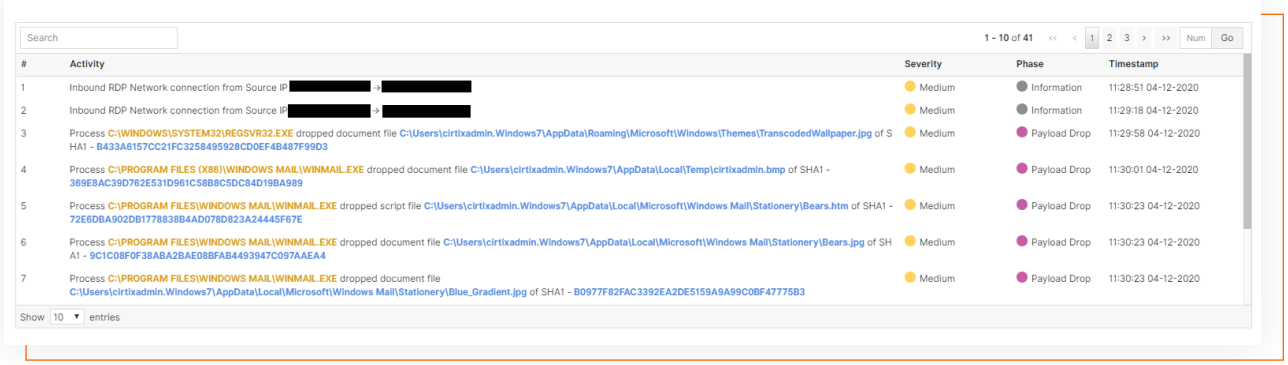
The Threatdefend platform will detect when the attacker tries to steal credentials using tools like Mimikatz and BlackEnergy. Post-detection, the platform forwards alerts, events, warnings, and logs to most of the popular Security Incident and Event Managers. This capability supports existing incident response processes and workflows, reducing the operational overhead associated with introducing a new security control, but forwarding the events is only half of the story.

The platform then enriches the data by querying other sources for information. Once the platform sends the query to the SIEM, it gathers all the resulting data involved in the event, thereby enriching, correlating, and validating it to make the alerts more useful and actionable. The Attivo Networks solution supports dynamically querying for the use of deceptive objects across the organization. If required, the BOTsink or Attivo Central Manager (ACM) can also export the decoy objects in standard formats to import into the SIEM, and then write rules in the event aggregator.

The example below shows the attacker's login activity, the activity post-login, and analysis of the payloads dropped:



	Severity	Attack Phase	Timestamp	Service	Description
1	Very High	Deceptive Credentials	14:41:16 04-21-2020	NETWORK	**Deceptive Credential Usage Splunk Time=2020-04-21T14:30:53.000+05:30; Splunk Index=main; Splunk Source Type=syslog; Splunk Host=[redacted]** WinEvtLog: Security: AUDIT_SUCCESS(4624): Microsoft-Windows-Security-Auditing: (no user): no domain: Windows-7-64-2: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: Windows-7-64-2$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 10 New Logon: Security ID: S-1-5-21-3209721862-224874804-2760181321-1212 Account Name: a-u-w-rdp-0264l Account Domain: Windows-7-64-2 Logon ID: 0x114ae8f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x644 Process Name: C:\Windows\\System32\\winlogon.exe **NETWORK** Information: Workstation Name: Windows-7-64-2 Source Network Address: [redacted] Source Port: 38698 Detailed Authentication Information: Logon Process: [redacted] Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type","src_ip":[redacted]"src_category":"Deceptive Credentials","service":"WINLOGON","VLANID":"","forwarder":"","src_ip_domain":"automation-web","dest_ip_domain":"","type":"WINLOGON","dest_ip_list":"","dest_port":"","dest_ip_port":"","botsink_ip":[redacted]"src_hostname":"automation-web","src_mac":[redacted] src_usernames":[ )
2	Very High	Deceptive Credentials	14:41:16 04-21-2020	NETWORK	**Deceptive Credential Usage Splunk Time=2020-04-21T14:30:53.000+05:30; Splunk Index=main; Splunk Source Type=syslog; Splunk Host=[redacted]** WinEvtLog: Security: AUDIT_SUCCESS(4624): Microsoft-Windows-Security-Auditing: (no user): no domain: Windows-7-64-2: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: Windows-7-64-2$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 10 New Logon: Security ID: S-1-5-21-3209721862-224874804-2760181321-1212 Account Name: a-u-w-rdp-0264l Account Domain: Windows-7-64-2 Logon ID: 0x114ae8f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x644 Process Name: C:\Windows\\System32\\winlogon.exe **NETWORK** Information: Workstation Name: Windows-7-64-2 Source Network Address: [redacted] Source Port: 38698 Detailed Authentication Information: Logon Process: [redacted] Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type","src_ip":[redacted]"src_category":"Deceptive Credentials","service":"WINLOGON","VLANID":"","forwarder":"","src_ip_domain":"automation-web","dest_ip_domain":"","type":"WINLOGON","dest_ip_list":"","dest_port":"","dest_ip_port":"","botsink_ip":[redacted]"src_hostname":"automation-web","src_mac":[redacted] src_usernames":[ )
3	Very High	Deceptive Credentials	14:41:16 04-21-2020	NETWORK	**Deceptive Credential Usage Splunk Time=2020-04-21T14:28:49.000+05:30; Splunk Index=main; Splunk Source Type=syslog; Splunk Host=[redacted]** WinEvtLog: Security: AUDIT_SUCCESS(4624): Microsoft-Windows-Security-Auditing: (no user): no domain: Windows-7-64-1: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: Windows-7-64-1$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 10 New Logon: Security ID: S-1-5-21-67388025-2718364118-1415250971-1361 Account Name: a-u-w-rdp-0264l Account Domain: Windows-7-64-1 Logon ID: 0x1da57641 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x824 Process Name: C:\Windows\\System32\\winlogon.exe **NETWORK** Information: Workstation Name: Windows-7-64-1 Source Network Address: [redacted] Source Port: 55782 Detailed Authentication Information: Logon Process: [redacted] Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type","src_ip":[redacted]"src_category":"Deceptive Credentials","service":"WINLOGON","VLANID":"","forwarder":"","src_ip_domain":"automation-web","dest_ip_domain":"","type":"WINLOGON","dest_ip_list":"","dest_port":"","dest_ip_port":"","botsink_ip":[redacted] src_hostname":"automation-web","src_mac":[redacted] src_usernames":[ )



Search

1 - 10 of 41 « ‹ 1 2 3 › » Num Go

#	Activity	Severity	Phase	Timestamp
1	Inbound RDP Network connection from Source IP [redacted] → [redacted]	Medium	Information	11:28:51 04-12-2020
2	Inbound RDP Network connection from Source IP [redacted] → [redacted]	Medium	Information	11:29:18 04-12-2020
3	Process C:\WINDOWS\SYSTEM32\REGSVR32.EXE dropped document file C:\Users\cirtixadmin.Windows7\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg of SHA1 - B433A6157CC21FC3258495928CD0EF4B487F99D3	Medium	Payload Drop	11:29:58 04-12-2020
4	Process C:\PROGRAM FILES (X86)\WINDOWS MAIL\WINMAIL.EXE dropped document file C:\Users\cirtixadmin.Windows7\AppData\Local\Temp\cirtixadmin.bmp of SHA1 - 369E8AC39D762E531D961C58B8C5DC84D19BA989	Medium	Payload Drop	11:30:01 04-12-2020
5	Process C:\PROGRAM FILES\WINDOWS MAIL\WINMAIL.EXE dropped script file C:\Users\cirtixadmin.Windows7\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.htm of SHA1 - 72E6DBA902DB1778838B4AD078D823A24445F67E	Medium	Payload Drop	11:30:23 04-12-2020
6	Process C:\PROGRAM FILES\WINDOWS MAIL\WINMAIL.EXE dropped document file C:\Users\cirtixadmin.Windows7\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.jpg of SHA1 - 9C1C08F0F38ABA2BAE08BFAB4493947C097AAEA4	Medium	Payload Drop	11:30:23 04-12-2020
7	Process C:\PROGRAM FILES\WINDOWS MAIL\WINMAIL.EXE dropped document file C:\Users\cirtixadmin.Windows7\AppData\Local\Microsoft\Windows Mail\Stationery\Blue_Gradient.jpg of SHA1 - B0977F82FAC3392EA2DE5159A9A99C0BF47775B3	Medium	Payload Drop	11:30:23 04-12-2020

Show 10 entries

For example, APT3 uses tools like BlackEnergy to dump credentials from multiple data stores like email clients, Windows Credential Stores, browsers, etc. The attackers use these stolen credentials on production servers to compromise, gather, and exfiltrate data. The platform detects the attackers when they use these deceptive credentials, thereby creating logs on the SIEM, which the platform can correlate to identify from where the attackers stole the credentials and how they gained initial access.

API-BASED QUERIES

The ThreatDefend platform supports automatically querying objects for most of the popular SIEM products offered, including but not limited to:

- Micro Focus ArcSight
- IBM QRadar
- Splunk
- LogRhythm etc.

The query to an integrated SIEM includes the following information:

- Decoy users
- Decoy names
- Email addresses configured for monitoring
- File Hashes for detecting data exfiltration on network boundaries

The platform offers integrations beyond querying the SIEM with other security controls to accomplish automatic isolation and threat hunting, which later works will cover.

CONCLUSION

Attivo ThreatDefend platform gives you complete coverage across the kill chain to detect, prevent, and automatically remediate the threats. Finally, it enriches the events across the kill chain to give deep insights into the attackers' TTPs to proactively uncover threats, improve Incident Response and mitigate future threats leading to maturity in the organization's threat hunting and response methodologies.

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