kuppingercole ANALYSTS

Exeon Trace NDR

John Tolbert

March 23

EXECUTIVE VIEW

Network monitoring is a foundational element of security architecture. Sophisticated attackers may deliberately delete logs on servers and endpoints to cover up their tracks. This means that the network, including private and public clouds, may be the last place that investigators can look to find evidence of malicious activities. Organizations need observability and the capabilities to take action at the network layer to better defend against cyber-attacks.

Content

Introduction

Commercial, government, and non-profit organizations of all kinds increasingly find themselves under cyber-attacks these days. Ransomware, fraud, credential theft, personal information and intellectual property leaks occur daily around the globe. IT teams mitigate the risks by employing and deploying a wide array of cybersecurity tools.

Network Detection & Response (NDR) solutions are designed to help security analysts discover evidence of current or past malicious activities on the network and/or in the cloud. NDR tools are effectively “Next-Generation Intrusion Detection Systems” (IDS). One of the significant differences between NDR and old IDS tools is that NDR tools use multiple Machine Learning (ML) techniques to identify normal baselines and anomalous traffic, rather than only static rules or IDS signatures. Given the volumes of network connection data that must be analyzed, using ML algorithms and models is a “must” rather than a “nice-to-have”. Historically, the major drawbacks to IDS were that it was labor-intensive to operate and could generate high numbers of false positives.

These security tools were created to discover and remediate certain types of attacks. Advanced Persistent Threats (APTs) are often perpetrated by actors from state intelligence agencies to gather intelligence on foreign companies and agencies, copying intellectual property, or sabotage. APT actors may also include well-funded but unscrupulous companies and hacktivist groups. Their goals often require long-term presence on victims’ properties, hence the use of the term “persistent”. APT groups have historically been the most likely ones to use Zero-Day exploits (those which were previously unseen in the wild), that may give them the advantage of not being detected by endpoint agents.

NDR has emerged as an additional tool to discover hitherto unknown compromises. Since data exfiltration is usually an objective of attackers, even in contemporary ransomware cases executed by cybercriminal units, properly deployed NDR tools can be better suited at discovering lateral movement from the initial compromised device to other assets within the target organization, use of compromised privileged credentials, and data exfiltration attempts. They can also help discover and remediate more common attacks such as unwanted bot activities, credential theft, and insider threats.

NDR tools are also deployed to provide visibility in OT/ICS/IIoT environments where it may not be possible to implement endpoint agent-based solutions. Enterprises often separate OT/ICS and IIoT devices onto their own networks for containment purposes. Such network segmentation is indeed useful, and the control points between these specialized networks and general-use and back-end networks are logical places to deploy NDR sensors.

NDR solutions can log all activities from attached networks in a central secure location for both real-time and later forensic analysis. They are usually implemented as a mix of appliances, virtual appliances, and IaaS VM images. Alternatively, some vendors take a more lightweight approach of receiving telemetry and optionally packet captures from network devices and analyzing and acting upon that, instead of in-line or using traffic mirroring deployment models. Proper design of NDR deployments is necessary to monitor all traffic flows.

A key differentiator for NDR is the employment of ML algorithms for detection. At a high level, unsupervised ML finds outliers or anomalies in traffic patterns; while supervised ML models categorize possible threats among the outliers, classify malicious activities, domains, and other attributes.

In terms of responses, NDR solutions can provide dashboards/alerts/reports, display real-time visualizations, allow drilldowns into details, enrich discoveries with threat intelligence, correlate events and provide automated analysis, halt suspicious traffic, isolate nodes, and send event data to SIEMs, SOARs, and forensic/case management applications. In cases where vendor products operate in passive mode, they direct 3rd-party security tools via APIs to execute these responses.

Product Description

Exeon Analytics was founded in 2016 in Switzerland. The company is a late-stage startup with multiple investors. Exeon's sales and support focus is in central Europe. Their network security monitoring product, ExeonTrace, originated from research conducted at the Swiss Federal Institute of Technology in Zurich.

There are three modules that comprise the product offering: network, web, and extended logs. Licensing costs are determined by the numbers of active IP addresses monitored and by the number of modules used. ExeonTrace is deployed on-premises or in the private cloud; there are no public cloud-hosted components. Exeon has professional services and system integrator partners in the region to assist customers with deployment.

ExeonTrace software is deployed as a virtual appliance on Linux servers on customer premises or in compatible customer IaaS cloud instances. It does not install off SPAN ports on routers/switches. ExeonTrace is a passive receiver of telemetry from network and other devices. ExeonTrace itself cannot capture packets or do Deep Packet Inspection, but it can be deployed together with partners' products for customers that need full packet capture capability. The enterprise management and analysis console run from the virtual appliance. Exeon does not host the console as SaaS, although they have partners that can do that if desired by customers.

The network module takes in various network flow information, among others NetFlow, IPFIX, DNS, firewall, switches and in general syslog information. It aggregates network flow data so that different logs sources are presented in a normalized structure to the analyst. It can also take as input logs from public cloud service providers. The web module collects logs from Secure Web Gateways (SWGs). The XLog module can be configured to ingest and process logs and alerts from a variety of sources, such as Microsoft Active Directory, CMDBs, DNS, EPDR systems, IDS, and VPN gateways.

ExeonTrace can indirectly analyze a long list of standard IP-based communications protocols, including DNS, HTTPS, ICMP, LDAP, RDP, SFTP/FTP, SMB, SMTP, IMAP, POP, SNMP, SSH, VIOP, IPsec, and BitTorrent. ExeonTrace does not have detection models specific to Operational Technology / Industrial Control Systems protocols but logs from those environments can be analyzed and fine-tuned. If requested, ingesting alerts from OT detection platforms can be integrated into ExeonTrace using partners' solutions.

ExeonTrace ships with static rules and ML-enhanced detection models. Exeon has developed their own unsupervised and supervised algorithms based on their own research, which are trained on open-source and partner data. ML detection models are updated as needed. It provides a framework allowing customers to leverage these ML algorithms to implement their own detection models. Customers work with professional services to put the proper models in place, baseline their environments, and set sensitivity levels for different areas within their environments.

For example, guest LANs will have different sensitivity levels than server LANs that contain confidential or mission-critical applications and data. This baselining and configuring process typically takes two weeks or less. These analyzers detect and classify malicious traffic according to MITRE ATT&CK®. Customers and/or Exeon professional services can use the built-in analyzers as templates to construct additional ones that are tailored to particular traffic types or environments.

ExeonTrace addresses the following use cases focused on network devices, endpoints, servers, and application behavior:

- Detection of malware compromise, 0-day vulnerabilities, and Domain Generation Algorithm (DGA
- Command and control traffic, DNS tunneling, botnet activity and port scans,
- Internal reconnaissance and lateral movement
- Identification of traffic by application, application behavioral analysis
- Discovery of specific attack methods, such as brute force attacks, Active Directory enumeration, association of user identity to traffic flows, and device fingerprinting
- Network analytics, such as aggregated network traffic volume analysis, time-based analytics, and endpoint-to-application utilization.

ExeonTrace looks at flow metadata only, which works even if the traffic is encrypted. It does not utilize techniques such as certificate analysis, HASSH, JA3/JA3S, or Mercury.

The solution correlates events from across customer's environments, assembles information into cases for analysts to investigate, and analysts can manually run queries against threat intelligence sources. Customers can configure API integrations with multiple threat intelligence feeds. MISP, STIX, TAXII, and YARA are supported.

ExeonTrace enables threat hunts with Indicators of Compromise (IoCs) both published and derived from observed behavior on customer networks. The analyst interface features drop-down query builders and regular expression searches. The dashboard shows timeline, map, and network map views.

Analysts can drill down into details from the dashboard to start investigations. The main screen shows an overview of anomalies, with severity scoring, and which endpoints are affected. By default, events are shown in the timeline view, with status of the case, IPs, domains, and ports/services. Analysts can filter by event, severity, IP address, or any other present field. Clicking on an IP shows a diagram of all the other IPs that the node in question has communicated with.

This allows investigators to see which communication pairings are abnormal and need further examination. Examples of anomalies that appear on the dashboard include external destination traffic, horizontal and vertical scanning, new service utilization on existing servers, unusual RDP client traffic, SSH, and using ports other than HTTP and HTTP(S) for web traffic. Context-specific information and investigators' notes can be entered and tracked for each case.

For the proxy module, analysts can see browsing trees that are built up from correlating multiple log files. Destinations are grouped by IP addresses to facilitate the determination of the extent of a possible incursion or data exfiltration event. Outlier detection helps at finding unusual behavior related to malware.

In terms of response actions, ExeonTrace is focused on alerting SOC managers and analysts over email or APIs. Playbooks are not present, but customers can script in alert conditions. It is possible for customers to build API integrations to external SOAR or XDR platforms. ExeonTrace does not generate root cause analyses or attribution theories. In addition to REST APIs, ExeonTrace supports CEF, SNMP, and syslog for integration with other security tools such as SIEMs and SOARs. Moreover, ExeonTrace can import data from SIEMs with ElasticSearch databases or any other type of log file. Exeon can analyze this imported data in conjunction with the network telemetry it collects through its matrix of ML detection algorithms.

ExeonTrace provides standard reports for customers. However, customers cannot create new report types within the platform. For additional reporting capabilities, customers can export the data and analyze it with other specialized solutions.

For customer analyst, investigator, and management access, ExeonTrace interoperate with LDAP directories and authentication services. Basic username/password authentication is the default. Depending on the authentication mechanisms present in the customer environment, strong and/or Multi-Factor Authentication (MFA) can be set up.

Since ExeonTrace is not a cloud-based service, customers can deploy and add storage as necessary and adhere to any data storage residency requirements as needed.

Strengths and Challenges

ExeonTrace is a lightweight network security monitoring solution that does not require the deployment and maintenance of physical appliances. It installs as VMs on Linux servers on customers' premises or private clouds. Exeon has developed proprietary unsupervised and supervised ML algorithms for detecting and classifying anomalous behavior on customer networks.

The management and analyst interfaces are intuitive and can yield important insights for customers. Exeon's approach to data retention helps customers keep data local for regulatory compliance and reduces cost for long-term storage by only retaining event metadata. The solution supports the most pertinent standards for exchanging threat information.

The company is relatively new. Hosting the enterprise console as a public cloud-based service may be advantageous for some customers. The response capabilities need further development beyond alerting. ExeonTrace's architecture focuses on API triggers to integrate in the customers' existing tool landscape. However, the addition of playbooks would help customers with responding to security events. Though MFA can be configured, it should be mandatory by default. Pre-built connectors for ITSM and SOAR would likely be useful for customers deploying in well-established enterprise environments.

Organizations that need network security monitoring solutions should take a look at ExeonTrace.

Strengths

- Physical appliances and network sensors not needed.
- Uses multiple advanced machine learning detection models.
- Can detect anomalies and malicious behavior without requiring packet decryption.
- Solution stores only metadata for more cost-efficient operation.
- Integration of various log formats and peripheral systems.

Challenges

- Responses limited to alerting via email or API.
- Playbooks are not available.
- Password authentication by default.
- No cloud-hosted SaaS options.

Related Research

Leadership Compass Network Detection & Response

Buyer's Compass Network Detection & Response

Leadership Brief: Do I Need Network Threat Detection & Response

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.