

genudetect

Network Detection & Response

genua.



Facts und Features

Definition

genudetect is a network detection & response (NDR) solution for the real-time detection of cyberattacks and anomalies in IT and OT networks. The solution passively analyzes network traffic using deep packet inspection (DPI), combines behavioral and signature-based detection methods, and provides complete visibility regarding communication relationships.

Through prioritized alerting, AI-powered attack explanations, and optional threat hunting, genudetect supports security teams in the rapid detection, analysis, and tracking of threats. Seamless integration into existing security platforms, combined with support for implementing BSI requirements for attack detection systems and the NIS2 Directive makes genudetect a powerful solution for modern enterprise and critical infrastructure environments.

Reasons to Choose genudetect

- Intelligent threat detection using combined analysis methods
- Context-based processing of security events for efficient response
- AI-powered support for attack analysis and assessment
- Flexible integration into existing IT and OT security architectures
- Efficient workflows through intuitive operation and optimized alert handling
- GDPR-compliant solution
- IT security made in Germany

Typical Use

- Monitoring of internal IT and OT networks for the early detection of cyberattacks and anomalies
- Securing critical infrastructure, government agencies, and enterprises in accordance with BSI requirements for attack detection systems
- Visibility of network communication and assets for security assessment and rapid incident response
- Integration into existing SIEM and SOAR environments to optimize established security processes
- Retrospective analysis of attacks via threat hunting to trace root causes, propagation, and impact

Customer Service

- Customer service directly from the manufacturer
- Security system management
- Hotline service
- Comprehensive training courses

SecurITy
made
in
Germany

Detection Capabilities

Detection mode	genudetect is operated as an IDS connected to a mirror port or a tap device
IDS	Suricata 5 and 7 compatible IDS engine
IDS rules	• genudetect ships with a powerful set of detection rules • Users can add additional and custom rules for enhanced detection
IoC	Detection of IoCs in the following formats: • IPv4 source address • IPv4 + port destination address • Domains • URLs
IoC data	• genudetect ships with a powerful set of IoC detection data • Users can extend this list with additional and custom IoCs for enhanced detection
New assets	Detection of previously unrecognized assets
Malicious SSL connections	Detection of known blocklisted SSL certificates
C2 traffic	Detection of command & control and botnet traffic using JA3 fingerprints of the SSL/TLS certificates

Processing Threat Detections

Streamlined SOC UI	The SOC admin can process all detections in dedicated and streamlined UI to perform this task efficiently
Collapse similar threats	Similar threats are grouped together and can be processed in a single step
Threat details	The following information will be shown for each threat: • Timestamp • Priority of the threat • Threat type and details • IDS rule in easy readable format • Communication partners with asset details for internal participants • Geo-IP information • MITRE tactics and techniques (AI assisted) • MITRE tactics and techniques short explanation (AI assisted)
Context information	The following information will be shown in context of a threat: • Frequency of similar threat hits • Previous similar detections • Other detections between the communication members
Mitigation support	Where possible, easy to understand mitigation information is provided (AI assisted), covering: • An explanation of the threat • Short term measures to address the threat • Final steps to resolve the underlying issue • Links to further information about this threat
Disable IDS rules	The use of IDS rules can be permanently disabled
Suppress threat events	Specific IDS rules can be permanently disabled by the user

Asset Management

New asset learning	Learn about new assets in communication
Asset attributes	The asset details originate from both communication and the CMDB data import
Asset criticality	Assets have a criticality level that is initially calculated heuristically and can subsequently be corrected manually or via an import from the CMDB
CMDB data update	Asset data can be updated automatically via a CMDB data import from a URL or an uploaded file

Threats Data Management

Supported threats data	genudetect supports the following threat data: - IDS rules in Suricata format 5 and 7 - IoC data as text lists in the following format: - IPv4 Source address, IPv4 + Port destination address, Domains, URLs
Supported IoC categories	genudetect supports the following IoC categories: - Command & control - Malware distribution/dropper hosting - Phishing - Spam/phishing mail server - Botnet nodes - Proxy/anonymising infrastructure - Drive-by download - Data exfiltration endpoints - Cryptomining pools - Bulletproof hosting - Sinkholes - Other/unspecified
Data source	System supports scheduled downloads from a web resource as well as manual uploads for air-gapped environments
Data source authentication	The following methods for authentication to fetch a datastream are supported: - None - URL secret - Basic authentication - API key

Reporting

Dashboard	System status via dashboard for threats and operation data
Threats report	Report of all recently found threats can be exported in .csv format
Asset report	Report of all known assets can be exported in .csv format
Sensor report	Report of all configured sensors can be exported in .csv format
Audit log	Report of all admin activity can be exported in .csv format
Error log	Report of all operation errors can be exported in .csv format
General table export	All tables in genudetect UI offer a .csv export

Data Export

Data sources	The following data can be exported - Confirmed threats - Raw threats - Audit logs - Error logs
Data export targets	The following export targets can be configured - SIEM - Mail (via SMTP) - MS Teams - Webhook
SIEM export options	SIEM export supports the following variants and formats: Variants: - RFC 3164 (BSD syslog) - RFC 5424 - CEF (Common Eventlog Format) Formats: - EVE-JSON - JSON - CSV - STIX 2.1

System Monitoring

genudetect Sensor Status

genudetect Nexus status	Sensor connection status visibility in sensor management
Error counters	Display of processing statistics and error counters to detect overload conditions
Syslog	Export of all syslog data to an external syslog sink using RFC 5424-compliant syslog via UDP, TCP, or TLS
SNMP traps	Critical events on the sensor generate SNMP traps

genudetect Nexus Status

Dashboard	The genudetect dashboard provides an overview of the genudetect operation
Error log	A log of all errors during operation lists all issues which happened while no one was logged in
Error log export	The error log can be exported to a configured SIEM
Prometheus	Various parameters of genudetect operation can be accessed via prometheus and e.g. be displayed in a Grafana dashboard

Administration

General

User interface	Comprehensive Web UI in German and English language
Inline help	Additional help is available via an icon next to various settings in the user interface
Online documentation	Searchable HTML documentation provides quick help
Data retention	Configurable rules to purge internal data after 180-360 days for: • Audit log • Error log • Threats

User Management

IdP connection	User management via integration with MS Entra and Keycloak
Role support	Supports 4 different roles: • Super admin • Admin • Soc analyst • Auditor
Password rules	Internal passwords rules: • Length • Expect uppercase character • Expect lowercase character • Expect digit • Expect special character

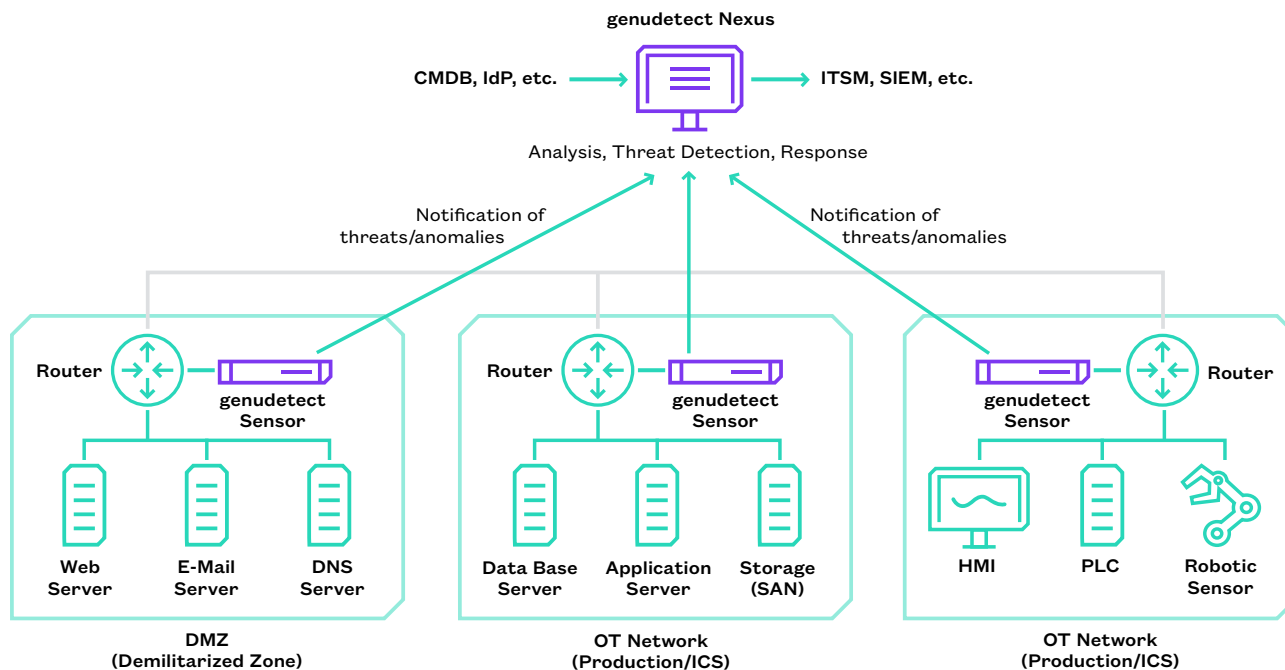
Installation

genudetect Nexus installation	Helm chart based installation on Linux PC with K3s (Kubernetes) running (further information in the release notes)
Sensor HW installation	Installation and configuration with comprehensive CLI
Virtual sensor installation	Installation and configuration with comprehensive CLI on KVM based hypervisors (further information in the release notes)

Backup

Backup tool	Command line tool for a scheduled export the system database as a Linux file or filestream to integrate with the user's backup system
-------------	---

Use Case



Network Monitoring of Multiple Locations

genudetec enables the central evaluation of data collected and transmitted by sensors distributed across various locations. This information is analyzed to detect threats and determine appropriate measures. A modern GUI provides administrators with a clear, real-time

overview of the monitored networks, allowing them to respond quickly to threats and anomalies based on recommended actions. In addition, the solution allows the seamless forwarding of threat intelligence to SIEM and SOAR platforms.

Further Information:

www.genua.eu/genudetec

All information in this data sheet is provided for product description purposes only, does not constitute a guarantee, and is not intended to be exhaustive. Technical changes are reserved. Actual performance may vary depending on the operating environment and configuration. Reproduction and/or duplication – including in part and/or in modified form – is permitted only with the written consent of genua.

genua GmbH

Domagkstrasse 7 | 85551 Kirchheim | Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu