

Anatomy of a Threat Report



Introduction

How much visibility do you have into what is happening on your network? Which devices are communicating with each other, and what types of data are being transmitted to and from your network? Understanding your network's activities and identifying its risks and threats are crucial for protecting your entire organization and your suppliers, partners, and customers.

By proactively assessing your network's security status with automated risk and threat reports, you can identify vulnerabilities or cyberattacks that may have evaded your perimeter defenses. This proactive approach empowers you to address these issues before damage occurs, strengthening your cybersecurity strategy and safeguarding your organization.

Core Network and Ransomware Reporting

ThreatSync+ NDR includes a Network Threat Report and Ransomware Defense Report. Both reports start with a summary section that displays the entire network's overall risk score and trend. They then provide detailed information on various policies and controls actively monitored by the NDR system. Each sub-section shows the individual threat score and trend line for each policy or control being monitored, and if any gaps or failures are found, guidance on how to remediate them. These reports are easily customizable to meet the specific needs of organizations or cyber defense programs. Their purpose is to highlight existing issues and provide managers with a way to establish network defense goals and track progress and improvements toward them.

(WistchGuard	WatchGuard	WinchGuard	Threat Detection
Network Threat Assessment Report	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	Performance Beneficial Structure Beneficial Structure Image: Structure Image: Structure Image: Structure Image: Structure Image: Structure
 A state of the s	High Rade Orison	75 Top Network Threats	Smart Avert Summary Exercises of Search Avert Summary of Search Avert Summary of Search Avert Search Avert Spectra
Advance and experience in the second se	INDE FAIL STORY IN AN ALL STORY IN ALL STORY IN A STORY INTA STORY INTA STORY INTA STORY INTA STORY INTA STORY INTA STORY	NEW YORK INCOME NEW YORK I	Potting or Recorrelations: A Moly VAR W TO
bed or a sole index of the	Mit Live Ram your The set of the set		Namini Makasu Spaniki Qwa Mito Mukuti Image: Comparison of the
LAKON S RUMA CAMERA Margine S and a starting of the s	inductions that the induction of the ind		

Network Threat and Ransomware defense reports provide highly detailed assessments of what is happening inside your network. They are essential to your cyber defense program because they provide the information needed to understand your security posture and what steps to take to improve it. The specific information included will vary depending on the assessment findings but typically include:

- A list of all the security risks that were identified.
- The criticality level of each risk, typically classified as critical, high, or medium.
- A description of each risk, including the type, severity, and potential impact.
- Recommendations for removing each risk, such as installing security updates, removing malware, isolating devices, changing credentials, or configuring security settings.

Examples of specific security risks that may be identified in the assessment:

- Activity on unsecured ports
- Command and control detection
- Unauthorized remote access

Failed backups

- Unnecessary and unusual port activity
- Actively exploited vulnerabilities
- Open alerts
- Unidentified and high-risk devices
- Policy violations
- Malicious network activity
- SMB leakage
- Unusual VPN activity

75	Top Network Threats			
THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	1. Abusive, suspicious, or malicious site access detected 1.2 Activity to Blocked Countries Detect traits to countries blocked by your frewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran. North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.	2 0 10/21 11/03	O Days
70	7. Unnecessary or Unexpected Port Activity 7.5 Trails con High Ports Crossing Network Boundary High port to high port trails - a possible indicator of persispent activity in distance and activity and the persispent activity in distance and the persispent activity in the second activity and the activity are blacking in to part of preventing activity, are blacking in to part of preventing activity, are blacking in to part of preventing activity and blacking in the part of preventing activity activity activity activity activity activity activity activity activity activi	We recommend investigating what ports the triggering traffic was running on. If these ports are not available with applications you expect the set of available with applications you expect them at the forwall.	76 0 18/21 11/63	O Days
50	3. Command and Control Detection 3.4 Unauthorized Outbound SSH An unauthorized SSI connection has been detected from an internal device to an external domain.	We recommend routing all legitimate essenal SSH connections through a VPN and blocking all incoming activity on ports 3309 and 22.		🚫 0 Days

Folicy Alerts			OBJECTIVE 3. Command and Control Detection Detect maliclous Command and Control activity.			Not Compliant
F Weighted Alert Threat count of 318.0 to		HREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
548.7 Alerts Per day (Average of past 7 20) days)	162334 167772834 4617162834 8617162834	60	3.1 Anomalous Activity to Blocked Countries Detect when any anomalous events are detected communicating to Blocked Countries	We recommend configuring your firewall to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.	1 05/06	5/12 0 Days
Likespetchel Informat. External to Internal GRZ Most Common Policy Violations Thatesgives Allo monitory user internal of statisty policies that a sempetchel In your in the out shows the monitory of activity policies that a sempetchel In your in the out shows the monitory of activity policies that the monitory of the second		60	3.2 Beaconing Through Web API Possible automated beaconing activity through a 7rd party web service has been detected between an IP in your network and a remete location. This could indicate use the service of could indicate use the service of the service of the service activity.	We suggest quarantining any machines you suspect are running beaconing scripts as well as running anti- virus scens.		5/12 0 Days
uncer ponces on were acure using the penal 13 key = 19 key. Internal Server Dangs. 0 0 Critical Acues	500 1,000 1,500 2,000	50	3.4 Unauthorized Outbound SSH An unauthorized SSH connection has been detected from an internal device to an external domain.	We recommend routing all legitimate external SSH connections through a VPN and blocking all incoming activity on ports 3389 and 22.	0	5/12 0 Days
New Internal Mode Policy Alerts by Tags This chart shows the most common tags of alerts generated during the period 13 May -19 Mgr. Rassemant Prevento. 0.00000000 10	Unauthorized Traffic Service Continuity Raisonnaire Prevento	\bigcirc	3.5 Unexpected DNS Resolution Server Transform Internal and/points to memory and the server is detected. This may be an indication of using the DNS protocol for ransomware related Command and Control activities.	We suggest ensuring all devices in your network are configured with your authorized DMS server and disability DMS zone transfers to untrusted hosts. We also suggest investigating the volume of the DMS traffic that triggered these alerts to identify possible command and control or exfitzation activity.	05:006	5/12 182 Days

To learn more about the WatchGuard Network Threat Report and Ransomware Defense Report, please contact your WatchGuard representative.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit <u>WatchGuard.com</u>





www.gointernos.com

SALES 305-590-5333

Network Threat Report and Ransomware Defense Report are provided to you on an "as is" basis, with no representation or warranty of any kind, express or implied. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2024 WatchGuard Technologies, Inc. All rights reserved. WatchGuard the WatchGuard logo and ThreatSync are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67770_060424