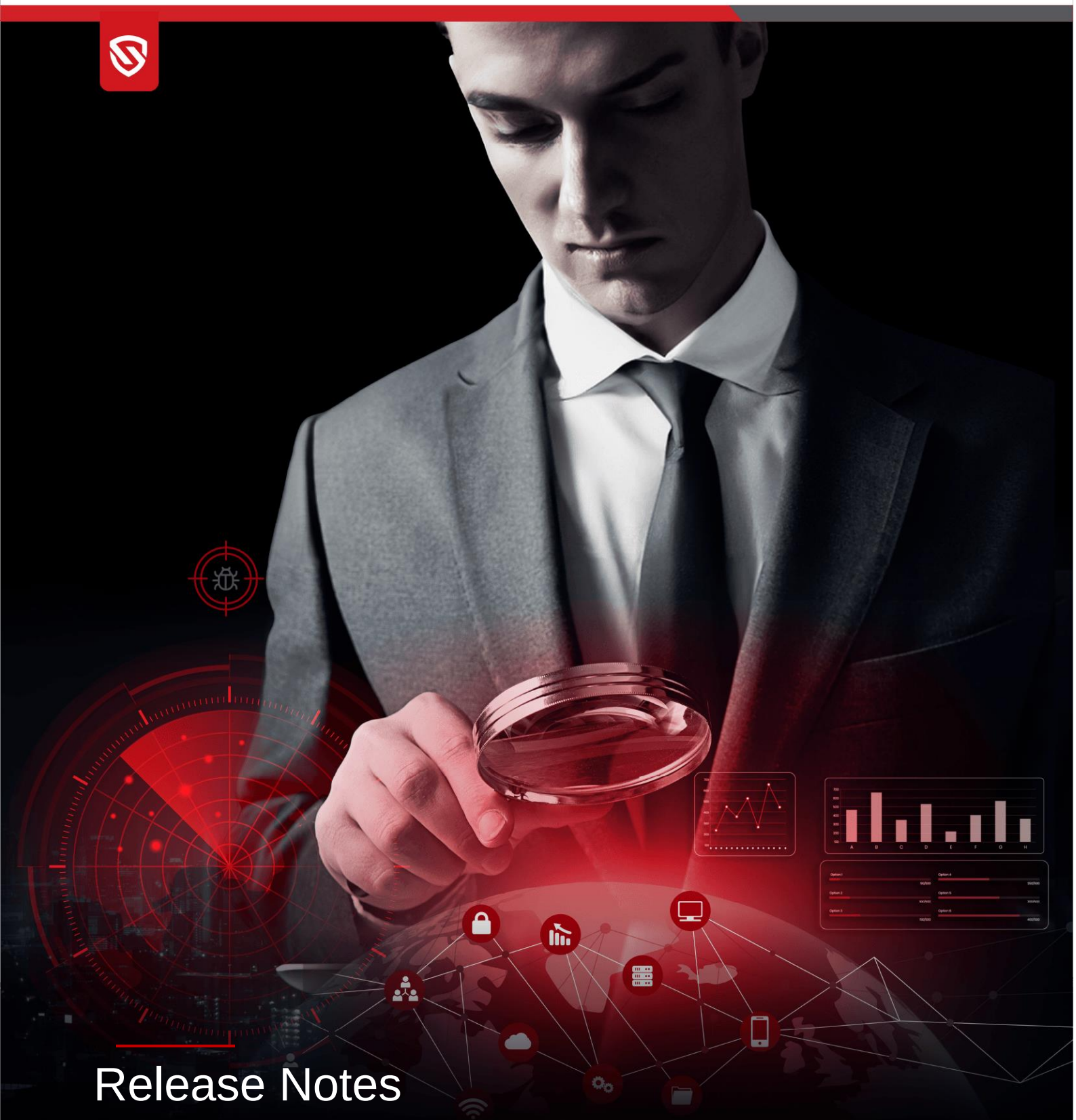
Seqrite eXtended Detection and Response

SEQRITE



Release Notes

v2.2

8 May 2024

www.seqrite.com

Copyright Information

Copyright © 2024 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

Trademarks

Seqrite is registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Content

Copyright © 2024 Quick Heal Technologies Ltd.

Seqrite XDR

Seqrite XDR, Extended detection and Incident Response Solutions, helps you monitor your network for any signs of active cyber threats and respond appropriately. Seqrite XDR facilitates proactive threat detection, investigation, and effective remediation to modern day cyber threats. Seqrite XDR supports threat hunting, system and custom alerts, detailed alert analysis and high-level reports that give you a bird's eye view of the organization's security posture. Seqrite XDR brings stability, reliability, security, and an intuitive UI.

Features released in Seqrite XDR 2.2

Introducing SKU: EDR Advanced

XDR has introduced a new version called EDR Advanced. It's a simpler variant focusing on essential features for a better user experience. Although it doesn't have Playbook and Connector features, it's crafted to provide focused solutions tailored to individual user requirements.

Super Admin Role

XDR introduces the Super Admin role, consolidating permissions from the existing SOC Manager and Admin roles for enhanced administrative capabilities.

Whitelisting for Network Incidents

XDR now offers whitelisting functionality for network-related incidents, providing users with greater control over incident response and management.

Manual Alert Generation

Users can now manually generate alerts from the existing process tree for detecting malicious activity, particularly useful when pre-defined rules are not available for certain scenarios.

Backend Update: Alert Cap Management

Now, managed alert caps in the backend: Set a maximum of 4000 alerts per rule every 30 minutes. If exceeded, rules deactivate automatically. Custom Rules notify admins, while System Rules inform Quick Heal's team.

Copyright © 2024 Quick Heal Technologies Ltd.

Enhanced Alert Validation with URL Reputation Checks

In this release, we've introduced URL reputation checks to validate alerts against predefined rules. Leveraging category classifications such as 24/34, we scrutinize URLs based on their content nature. Alerts matching rules and categorized within 24/34 are forwarded for further analysis. Conversely, alerts triggered by URLs outside this category or encountering errors like unapproved domains or invalid URLs are disregarded to prevent false positives.

DNS Protocol Capture Enhancements

CName and TXT Attributes: Now captured within DNS protocol, providing deeper insights into domain resolution activities.

Linux Sensor Improvements

Socket Events Capture: Socket events are now comprehensively captured, empowering better visibility into network communications on Linux systems.

Enhanced Sensor Coverage for Linux and macOS

USB Mount Events: Capture of USB mount events is now supported on both Linux and macOS sensors, bolstering endpoint visibility and security monitoring.

Copyright © 2024 Quick Heal Technologies Ltd.

Bug Fixes and Known Issues

Here are the bug fixes and known issues in version 2.2:

Bug Fixes

- A rare BSOD issue in DNS protocol capture has been resolved.

Known Issues

- In the case where the DNS response consists of multiple segments, the sensor will disregard it.
- Alerts are not being searched when using the filter "Rule Name=Manual Alert”.

Copyright © 2024 Quick Heal Technologies Ltd.

Usage Information

- Microsoft has deprecated support for SHA-1 and recommends using only SHA-2 signed certificates for its OS updates. Accordingly, the SHA-1 certificates that Seqrite was using expired on 4th June 2021, so the following operating systems are not supported unless the appropriate patches are applied.
  - Windows Vista – Not supported
  - Windows Server 2008(below R2) – Not supported
  - Windows 7. To continue using this operating system without any issues, please apply "KB4474419" and "KB4490628" service packs.
  - Windows Server 2008 R2. To continue using this operating system without any issues, please apply "KB4474419" and "KB4490628" service packs.
- All process events whose process create event is older than 30 days, return a "No data found" error in response and Alerts are not generated for these processes even though corresponding rule may exist.

Copyright © 2024 Quick Heal Technologies Ltd.

Technical Support

Seqrite provides extensive technical support for its users. In case you face any technical issue, you can contact our Technical Support center using the options available at the following URL:

https://www.seqrite.com/seqrite-support-center

Copyright © 2024 Quick Heal Technologies Ltd.