TRAPX SECURITY

DECEPTIONGRID™

v. 7.0

Release Notes

TrapX® Security, March 2020

trapx.com

Contents

Preface

TrapX Security® is pleased to announce the release of DeceptionGrid™ version 7.0. This is an important release including new features and resolutions of known issues.

Release Date: March, 2020

These release notes list new features and issues in DeceptionGrid version 7.0.

What's New in Version 7.0

The current release introduces the following new features and capabilities.

In This Section

Security Analysis and Reporting

- **Attack Intelligence**: You can now receive updates on newly-discovered threats, from TrapX analysis experts. The posts appear directly in TSOC, for customers who have opted to share their sanitized event data with TrapX analysts.
- **Real-time event reporting**: Emulation traps now report events as they occur, without waiting for sessions to close.
- **Scan-only exception**: Whitelist a connection, specifying to suppress only Scan-stage events including Ping.
- **Full OS trap file analysis**: Static and dynamic (sandbox) analysis of event binaries are now supported for Full OS trap events, in a similar manner to existing analysis for emulation trap events.
- **Triggers**: Trigger (email alert) configuration has been simplified.

Detection

- **Attacker discovery**: When possible, traps (Emulation and Full OS) discover the attacker's source operating system and MAC address. This information is then included in the event.
- **Ransomware detection**: With CryptoTrap enabled, Full OS traps intelligently detect ransomware behavior anywhere in the file system (not just in the CryptoTrap folder) and accordingly record an event.

Deception, Emulation and Deployment

- **High-Interaction SSH**: For ultimate realism and deception, the SSH service on relevant emulations can now be connected to a sandboxed full Linux OS, built into the DeceptionGrid Appliance but securely isolated from it. Attackers receive real responses to all relevant commands, and the environment includes all real OS components such as Linux kernel, file system and network connections.
- **Coverage analysis**: To facilitate educated trap deployment decisions, TSOC can now display information on trap coverage of organizational network subnets. You can configure the criteria for considering subnets adequately covered.

- **ForeScout CounterACT integration for Inventory**: For asset inventory, which can be used for trap automatic configuration and / or for coverage analysis (above), TSOC can now retrieve organizational asset information from the organizational Forescout CounterACT.
- **Kerberos support for SMB**: SMB emulations now support Kerberos authentication.

Enterprise Integration

- **TSOC SAML authentication**: For single sign-on (SSO) to TSOC, you can now integrate with your organizational SAML-based Identity Provider (IdP) such as PingFederate or OneLogin. Users log into the organizational system, according to whatever security protocols are organizationally required (for example, multifactor authentication), and are automatically authorized by TSOC according to their TSOC roles.
- **LDAP DN support**: You can now set the TSOC user authentication domain in Distinguished Name (DN) format, in addition to existing support for User Principal Name (UPN / email address) format. This enables integrating with organizational LDAP servers that do not support or are not configured for UPN format, such as OpenLDAP.
- **Event Syslog improvements**:
  - To facilitate automated event parsing, in the event Syslog cs3 (Custom String 3) field, which lists connections and commands used during an attack, pipes (|) now separate the individual connections and commands, each of which contains comma-separated key:value pairs.
  - Event Syslogs sent directly from Appliances are now enriched to match Syslogs sent from TSOC.
- **Exceptions dark mode**: When enabled, emulation traps do not respond at all to TCP connections from IP addresses for which an Exception is configured for all ports. This can be useful for preventing false-positive alerts from organizational scanners.

API / SDK / CLI

- **Windows-based CLI tool**: TrapX now provides a Windows-based CLI tool for TSOC API commands. You can use the CLI tool to run remote commands on TSOC, interactively or in a script.

  Developers now have a variety of options for implementing TSOC commands and scripts: Python SDK, Windows CLI (interactively or in script), and directly to the REST API.
- **Web imitation for trap customization**: Scanning an existing endpoint on which to base trap configuration (Build your own Trap - BYOT; from SDK or CLI tool) can now include scanning the endpoint's web service to emulate web content, using any of several supported tools.
- **Trap mass configuration**: Interactive tool for downloading, editing, and uploading an Appliance's entire configuration of interfaces and traps. Range-based syntax enables mass deployment.

- **Simplified event download**: A single SDK / CLI command now enables downloading full event information and associated binaries, according to specified event criteria. Using this single command is the equivalent of the combined three legacy commands for searching events, showing them, and downloading files.
- **TSOC shutdown**: API command for administrative, graceful shutdown of TSOC, such as for periodic backup or other administrative purposes.

Upgrade

In This Section

Upgrade Notes

For full functionality of this DeceptionGrid version's new features and resolved issues, it is required to upgrade TSOC and all Appliances and Full OS traps to version 7.0.

Upgrade to the current release is supported only from TSOC version 6.4.7 / Appliance version 6.4.7 / Full OS 1.3. Otherwise, you'll need to perform a two-step upgrade.

TSOC must be upgraded first, to be able to begin upgrading Appliances. Appliances of previous versions will not continue to work reliably with the current version of TSOC.

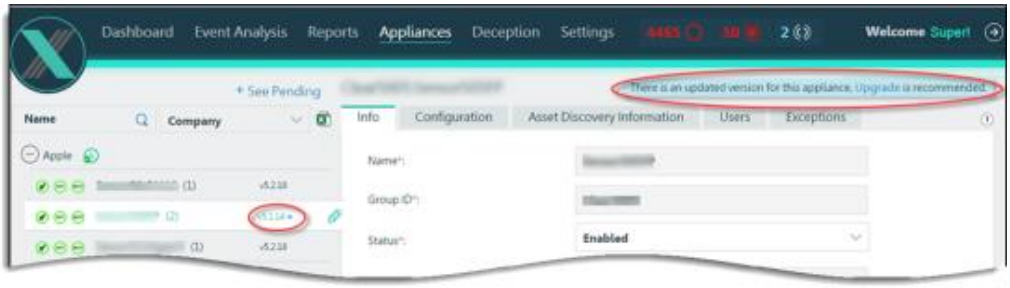
Before upgrading, make sure virtual hardware conforms to requirements as in the *DeceptionGrid Installation Guide* (unchanged from previous version).

Upgrade Instructions

To upgrade to the current release:

1. For extra security, it is recommended to save a snapshot of the TSOC server. If your Appliances are also virtual, save snapshots of them as well.
2. Make sure servers meet requirements as in Upgrade Notes above.
3. If at any point in the past any DeceptionGrid component was restored from a snapshot, restart that component.
4. Log into TSOC as a Super Admin.
5. In TSOC, click the upgrade message:

   Follow instructions until the process is complete, including the TSOC server being restarted.
6. In TSOC, go to **Appliances**. Appliances and Full OS traps that are not yet upgraded are marked with •, and upon selecting them, an upgrade message appears:



For each relevant Appliance, in the message click **Upgrade** and follow instructions.

7. After upgrading a full OS trap, return it to Active mode and create a new baseline snapshot.

Post-Upgrade Notes

If before upgrade you downloaded a Deception Token package for external distribution, to ensure compatibility with the upgraded TSOC and traps make sure to download a new package for distribution.

Resolved Issues

The following issues are newly resolved in this release:

Component	*Description*
TSOC	Event Syslog time stamps now conform to ArcSight CEF date & time format.
TSOC	When configuring a browser token, changes to the **Profile** are now saved.
TSOC	The dashboard now correctly displays Full OS traps on Windows workstations (7, 10).
TSOC	If an emulation type or OS version changes after an event, the event is now correctly displayed with the trap's original configuration.
TSOC	Files from Full OS trap SMB events can now be downloaded from the Event Analyzer on the first try.
TSOC	WebApp logs (Settings > Logs > WebApp) can now be exported to CSV.
TSOC	It is now possible to upload to web emulations web page zip files that are larger than 16MB (new limit is 256MB).
TSOC	It is now possible to configure spin data and authentication for SCADA FTP Monitor emulation.
TSOC	TSOC Administrators and Trap Managers can now perform all actions on already-configured Reports for relevant traps.
TSOC	Upon relevant events from emulated services proxied to a Full OS trap, automatic isolation of attacking endpoints (when TSOC is configured and integrated with organizational systems as relevant) now occurs.
TSOC	Syslog from TSOC upon an event from an emulated service proxied to a Full OS trap no longer records a superfluous event (for the connection from the Emulation trap to the Full OS trap).
TSOC	Initializing an Appliance no longer times out in cases of extreme overload on system or network.
Appliance	Packet captures (PCAPs) from HTTPS events now include correct attacker IP address and port.
Appliance	Emulation trap spin data (created via FTP to trap) can now have uppercase characters in folder and file names.
Full OS Trap	Connections to a full OS trap from the same source over different protocols are no longer grouped as one event.
Full OS Trap	Full OS traps now consistently record SMB events (anonymous connections).
Full OS Trap	SMB connections with Kerberos authentication to Full OS traps now correctly cause an event to be recorded.
Deception Tokens	The SMB Network Share token (for Emulation or Full OS trap) no longer produces false-positive events.
Deception Tokens	When browser tokens are distributed to Firefox, and on the endpoint an invalid duplicate profile exists, the tokens are now installed in the valid profile.
Deception Tokens	Installing browser tokens on an endpoint with unused Internet Explorer no longer causes the 'Set up Internet Explorer' window to remain open.

Support

Support for TrapX products is provided by TrapX or by an authorized TrapX Service Partner. More information and technical support for TrapX products are available at:

- support.trapx.com
- support@trapx.com
- Americas: 1-855-249-4453
  EMEA & Asia Pacific: +44-208-819-9849

Documentation Feedback

TrapX Security continually strives to produce high quality documentation. If you have any comments, please contact Documentation@trapx.com.

About TrapX Security®

TrapX Security is the pioneer and global leader in cyber deception technology, with flagship solution DeceptionGrid effectively detecting, deceiving, and defeating advanced cyber attacks and human attackers in real-time. DeceptionGrid provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. Deploying DeceptionGrid sustains a proactive security posture, fundamentally halting the progression of an attack. DeceptionGrid changes cyber-attack economics by shifting the cost to the attacker.

The TrapX Security customer base includes worldwide Forbes Global 2000 commercial and government customers in key industries including defense, healthcare, finance, energy, and consumer products. Learn more at www.trapx.com .

Disclaimer

Product specifications are subject to change without notice. This document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, TrapX cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be obtained by TrapX customers.

Trademarks and Copyright

Updated 25/3/20