

Practical ModSecurity Tuning

Christian Folini, netnea.com

SIGS Bern, 10. März 2015

F. Friedl

3 ARTEN VON WAF SETUPS

Naïve / Überforderte / Funktionierende

A black and white photograph of a muscular man with a mustache, shirtless, in a boxing stance. He is looking to the right, with his left arm extended forward and his right arm bent. The background is a plain, light-colored wall.

BLOCKING MODE

Komfortzone verlassen / Kämpfen / Lernen



MODSEC ERKLÄRT

Eingebettet / Hooks / Granulare Kontrolle



MODSEC CORE RULES

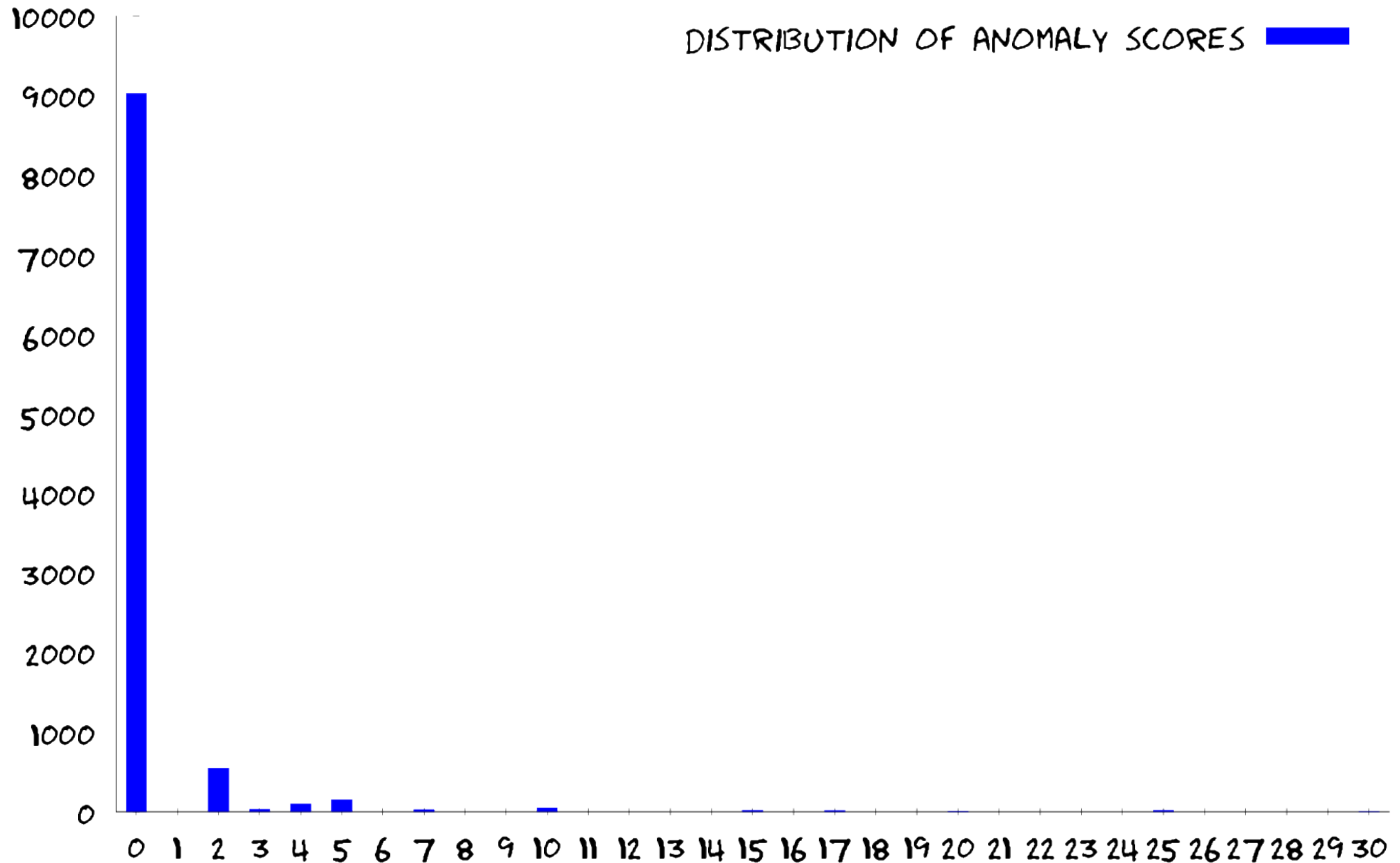
Limbo-Dance mit Usern und Angreifern



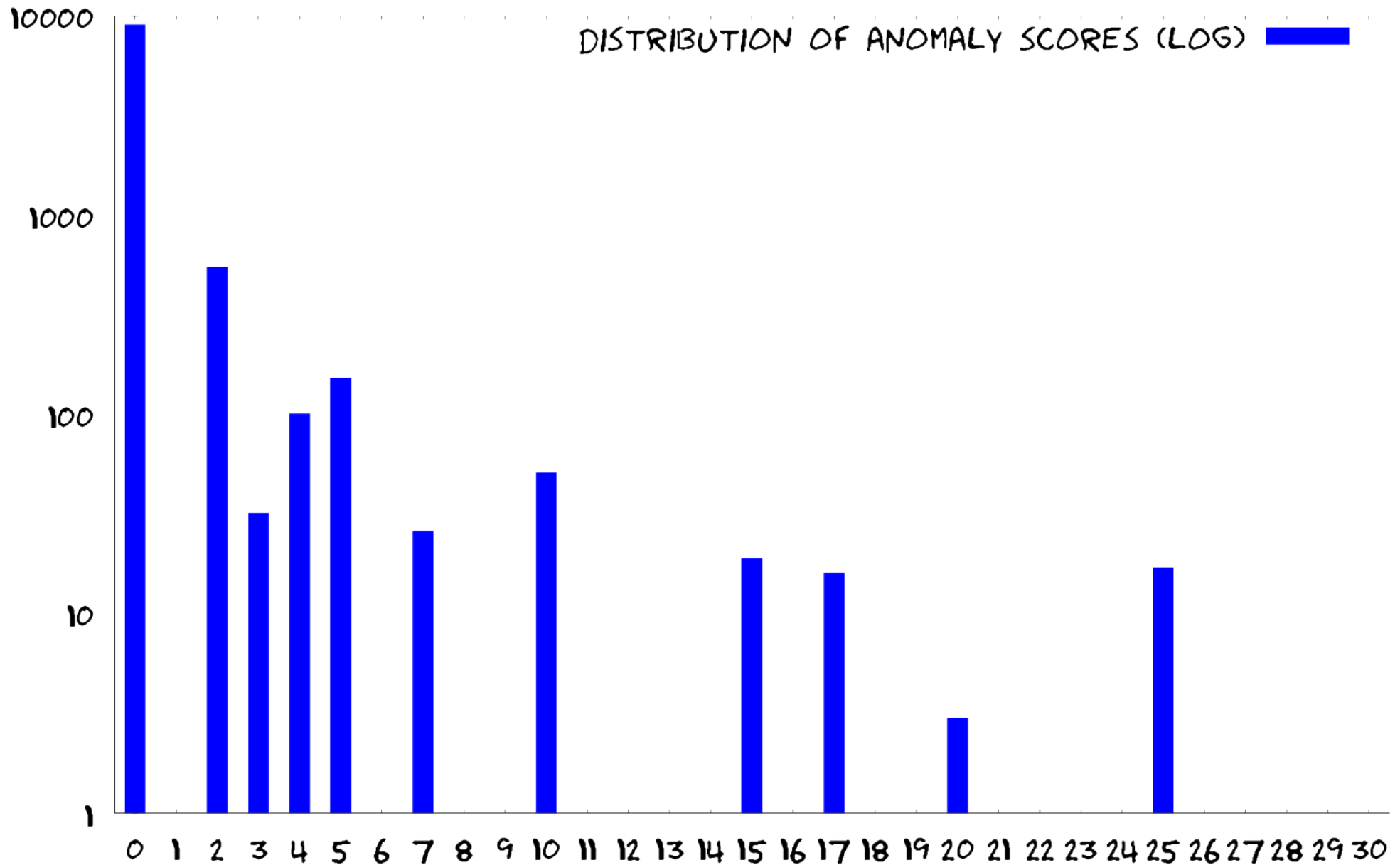
FALSE POSITIVES

LogFiles / Schritt um Schritt reduzieren / Sinnvolle Limiten

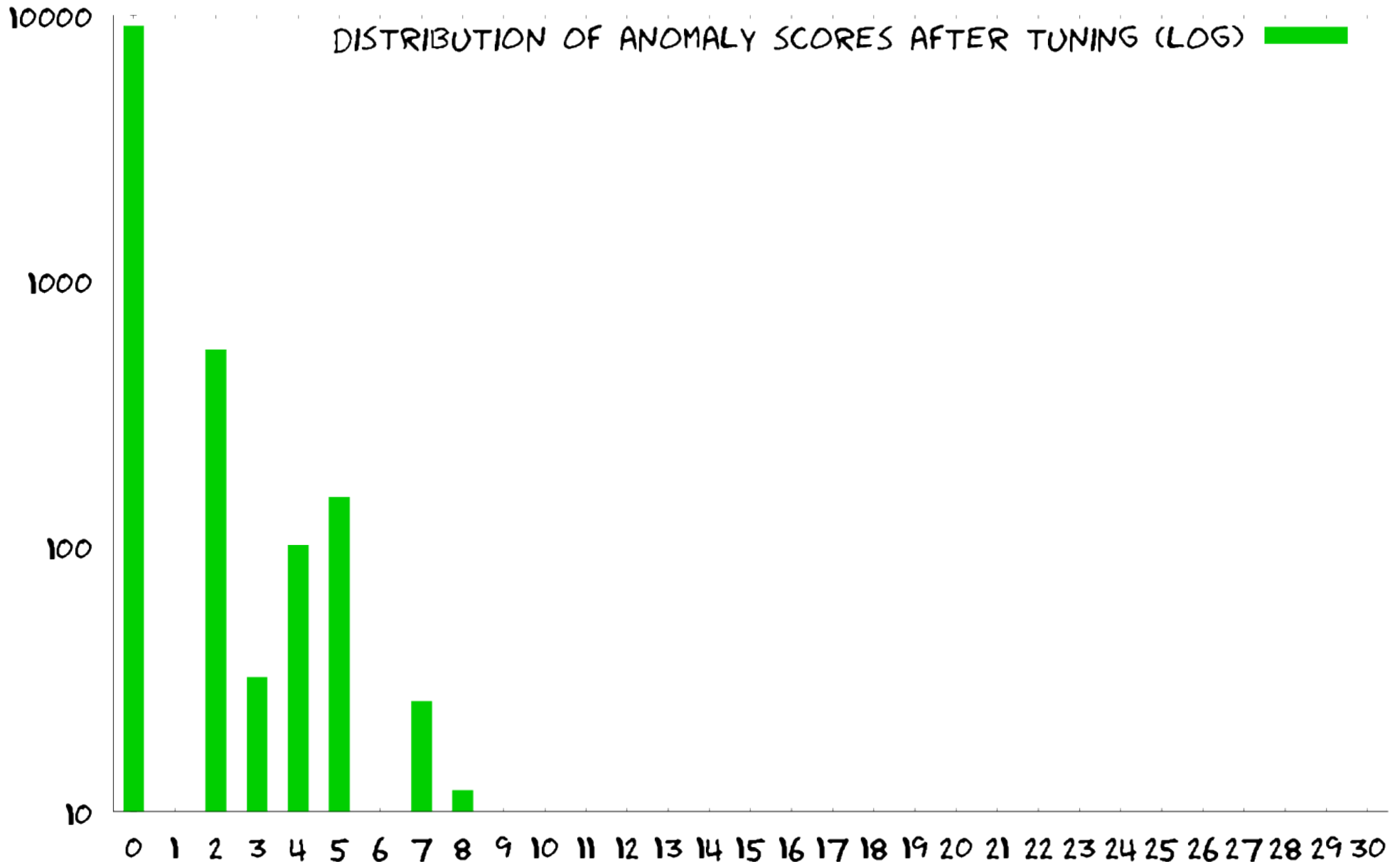
Anomaly Scores einer frischen Installation



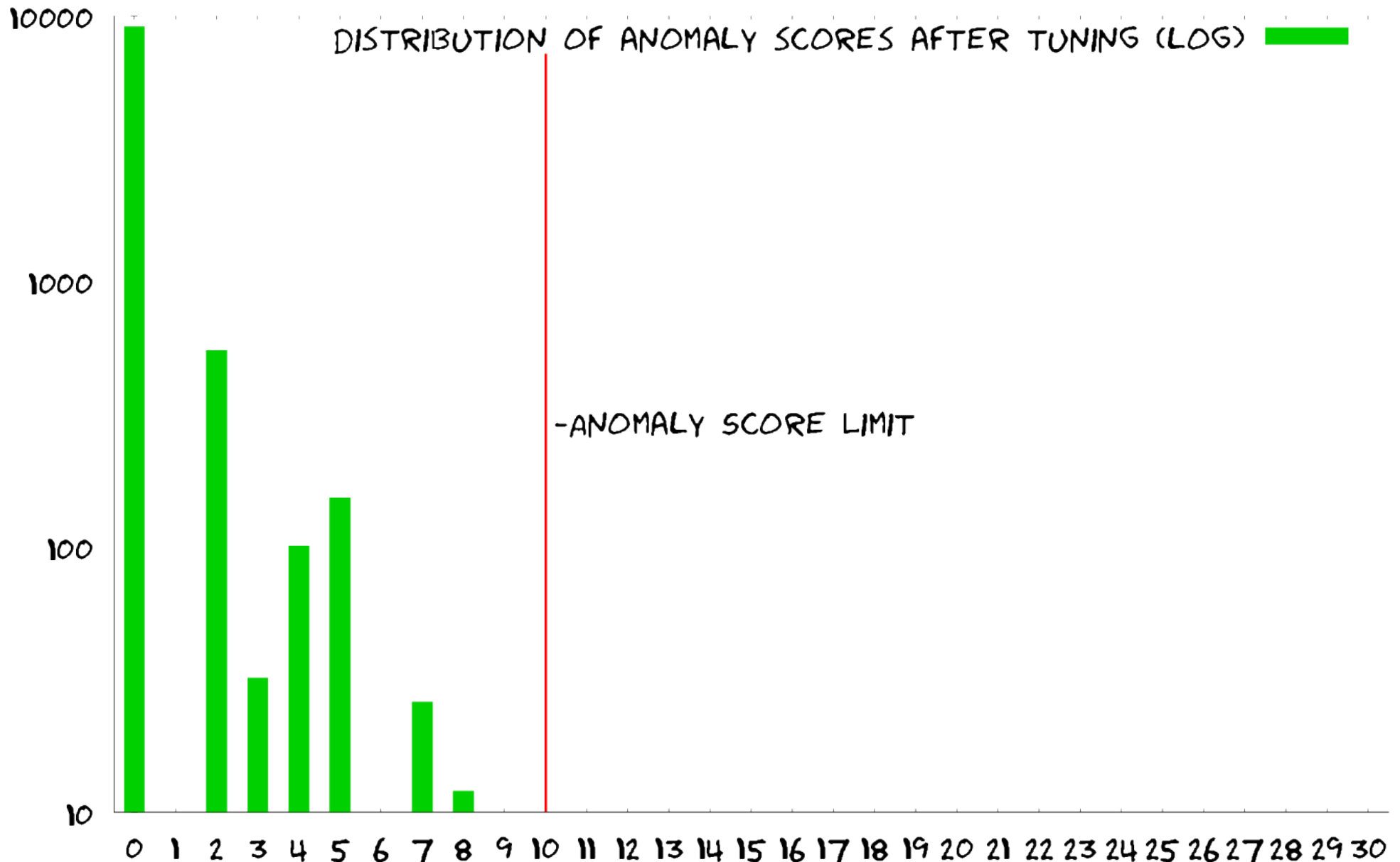
Anomaly Scores einer frischen Installation - Logarithmische Skala



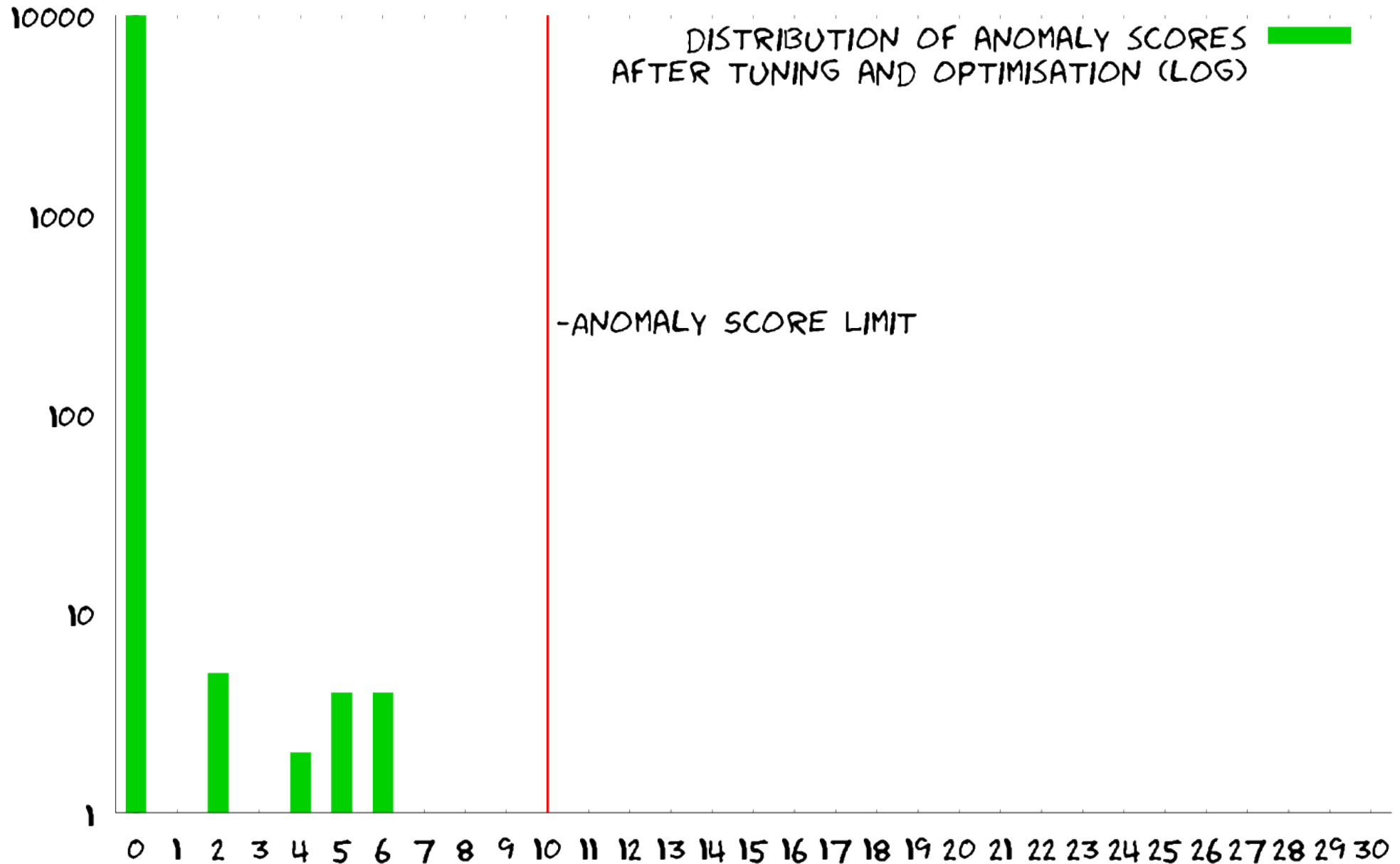
Anomaly Scores einer getunten Installation



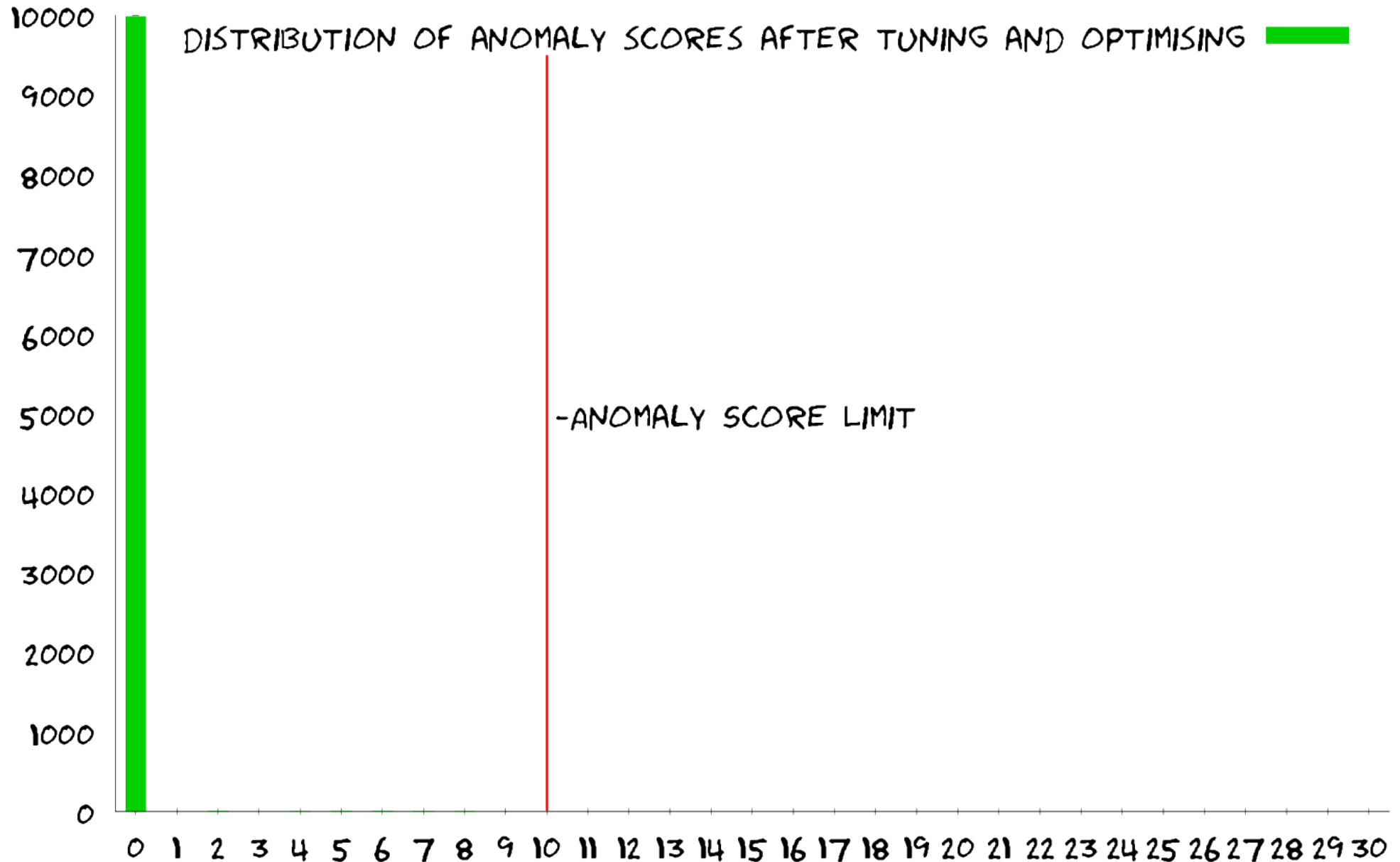
Anomaly Scores einer getunten Installation mit Limite

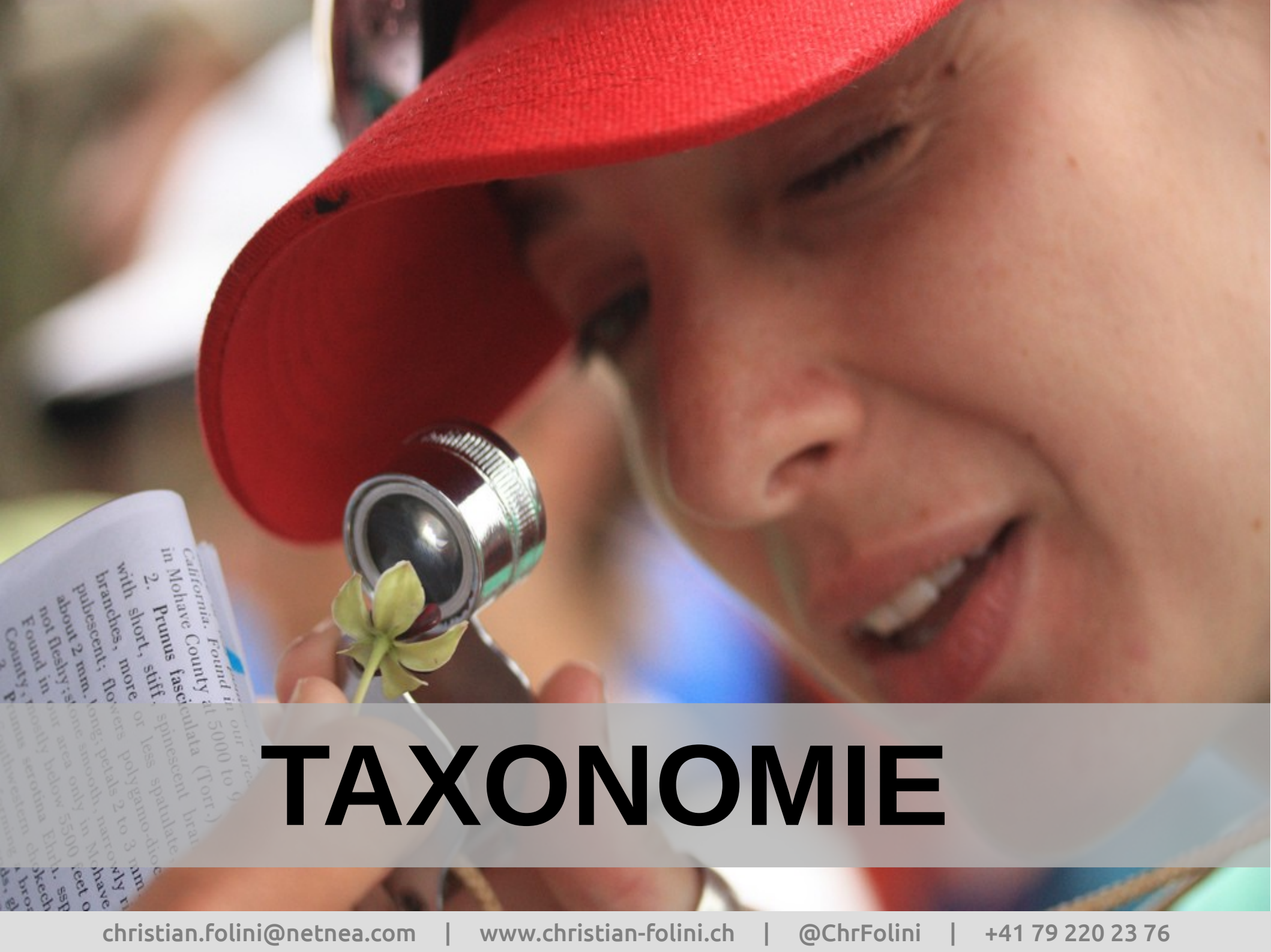


Anomaly Scores einer noch weiter optimierten Installation



Anomaly Scores einer optimierten Installation / Logarithmische Skala

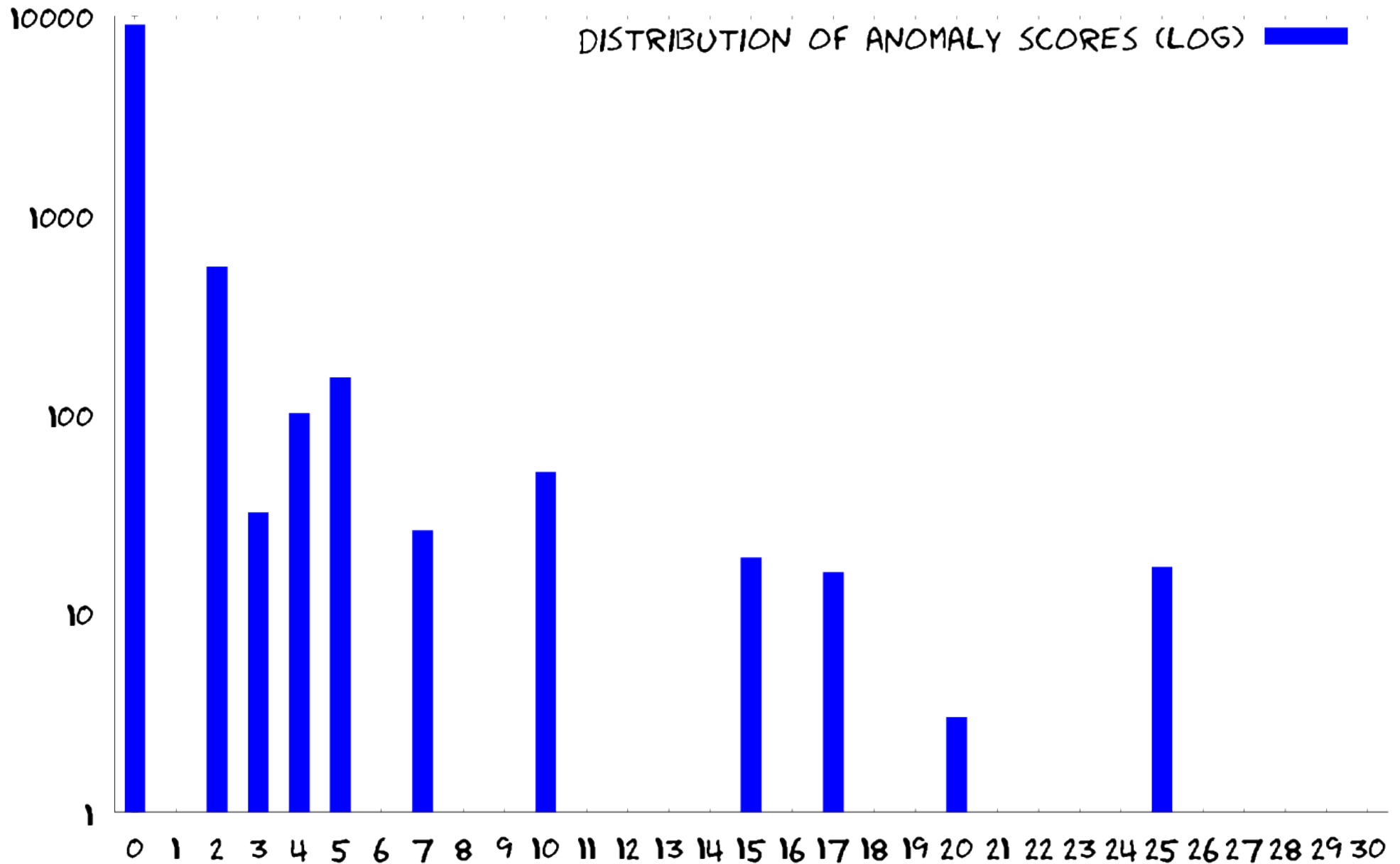




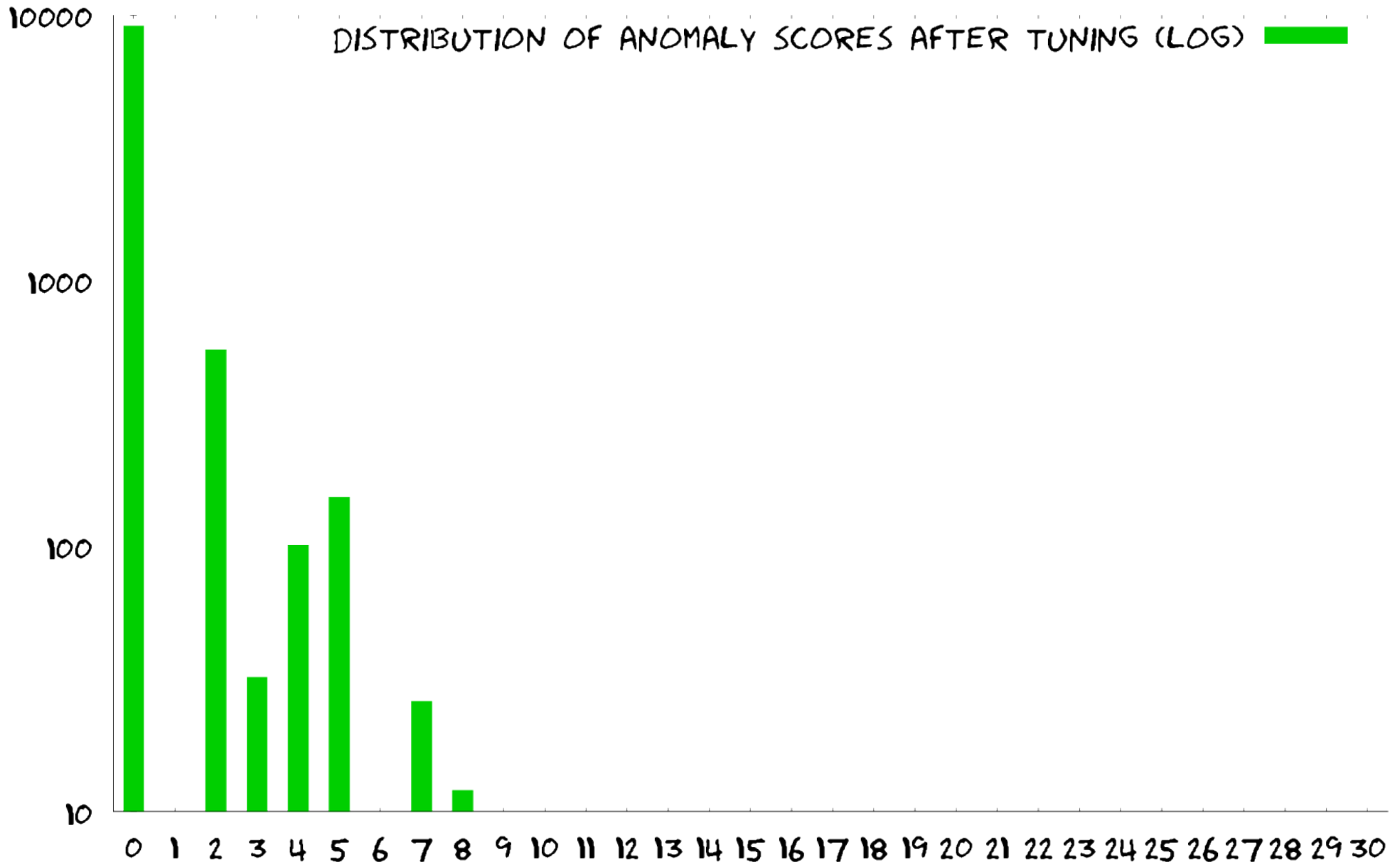
California. Found in our area
in Mohave County at 5000 to 9
2. *Prunus fasciculata* (Torr.)
with short, stiff, spinescent bran-
ches, more or less spatulate
pubescent; flowers polygamo-dio-
cous; petals 2 to 3 mm.
about 2 mm. long; petals 2 to 3 mm.
not fleshy; stone smooth, narrowly
Found in our area only in Mohave
County, mostly below 5500 feet o
Prunus serotina Ehrh. ssp
Southwestern chickadee
forming a brood
ids, gl

TAXONOMIE

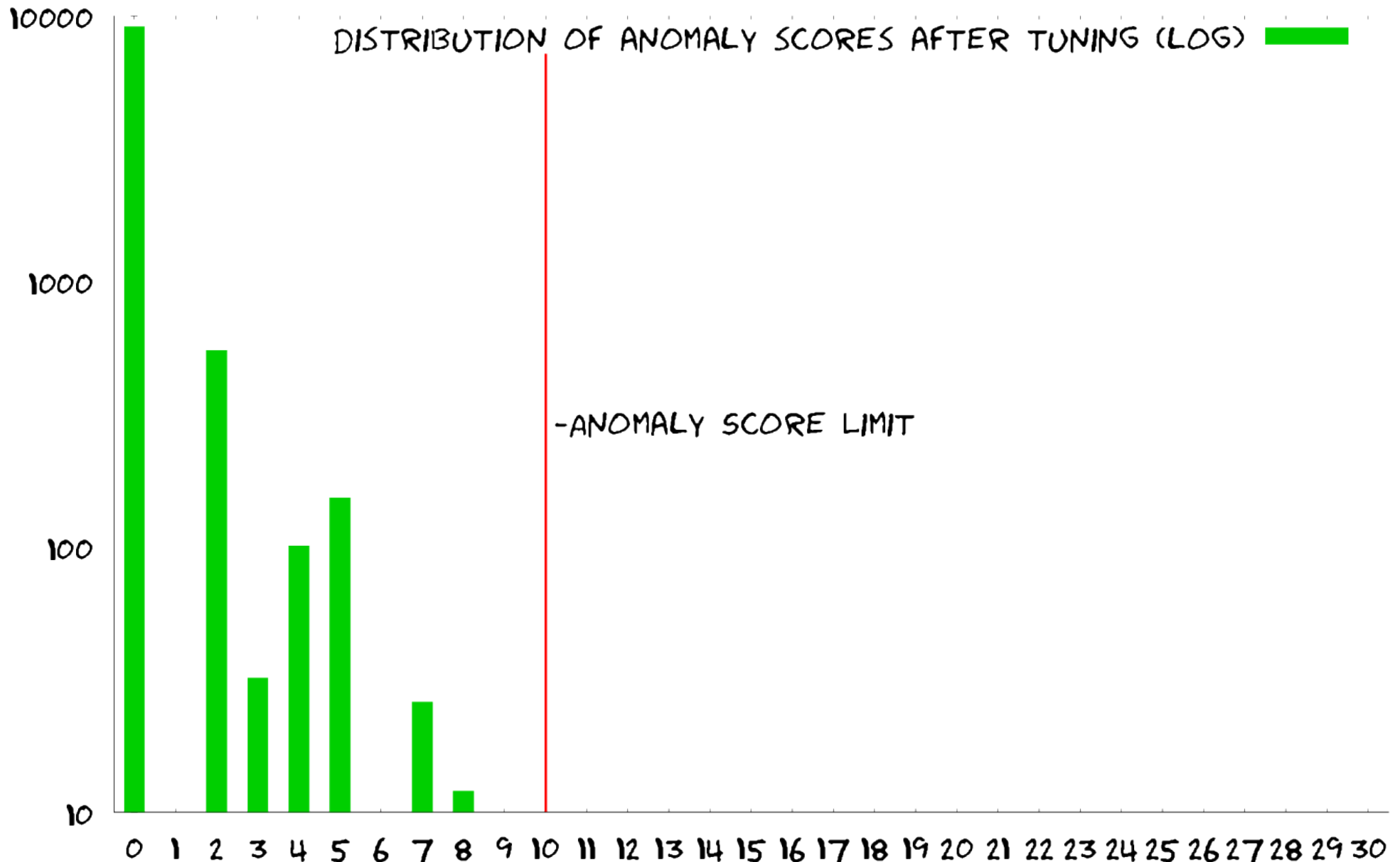
Anomaly Scores einer frischen Installation - Logarithmische Skala



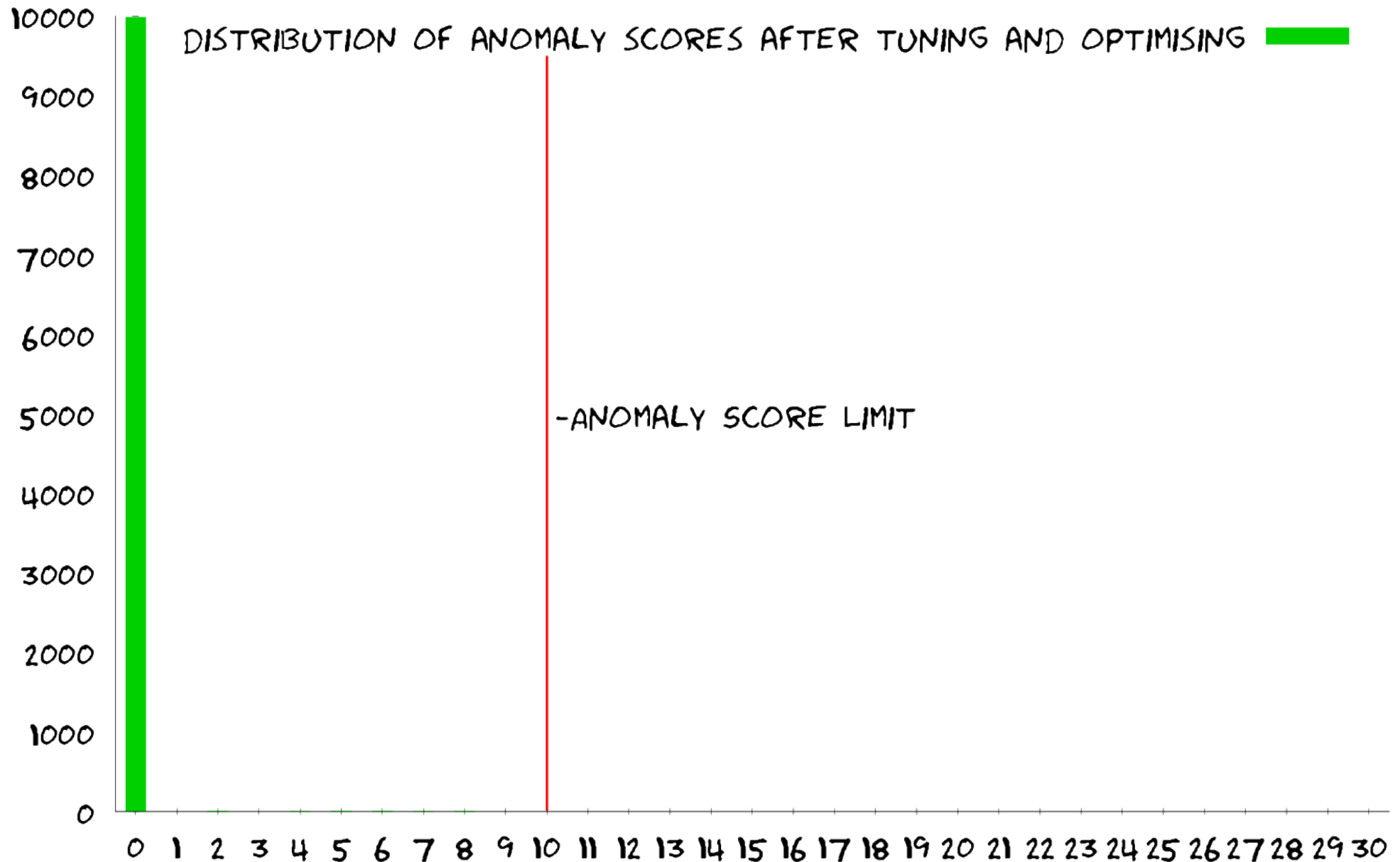
Anomaly Scores einer getunten Installation



Anomaly Scores einer getunten Installation mit Limite



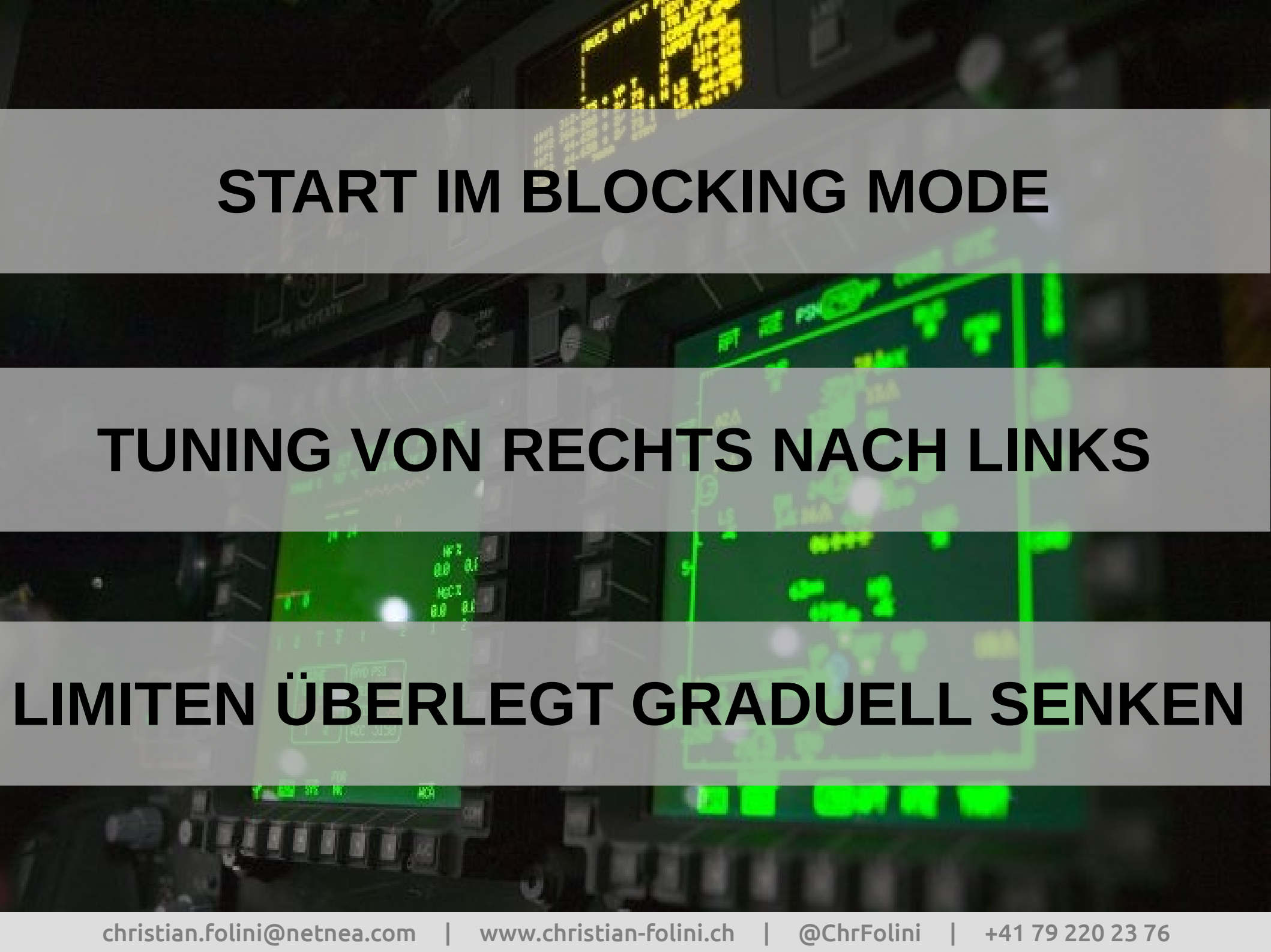
Anomaly Scores einer optimierten Installation / Logarithmische Skala





REAL LIFE DEPLOYMENT

2 Dozen Rules / Right Toolset / Config Mgmt is Key



START IM BLOCKING MODE

TUNING VON RECHTS NACH LINKS

LIMITEN ÜBERLEGT GRADUELL SENKEN

Photo Sources (all licensed via Creative Commons or in the public domain)

Discovery: <https://www.flickr.com/photos/flowtastic/13385797723> (by Florian F. / Flowtography)

Overly Manly Man: Public Domain

Watch: <https://www.flickr.com/photos/billadler/391674817> (by Bill Adler)

Star Wars Limbo: <https://www.flickr.com/photos/jdhancock/3605011903> (by JD Hancock)

Archive: <https://www.flickr.com/photos/londonmatt/9420645961> (by Matt Brown)

Taxonomist: <https://www.flickr.com/photos/11065470@N03/3691475990/> (by Nelson Stauffer)

Chinook: <https://www.flickr.com/photos/usairforce/5537364574> (by US Air Force)

Apache Cockpit: <https://www.flickr.com/photos/defenceimages/5038245563> (by UK Ministry of Defence)

Scripts and Aliases: www.netnea.com

Dr. Christian Folini

christian.folini@netnea.com

www.christian-folini.ch

@ChrFolini

+41 79 220 23 76

SIGS Bern, 10. März 2015