



Zurück zu den Grundlagen – Schwierig geht auch!

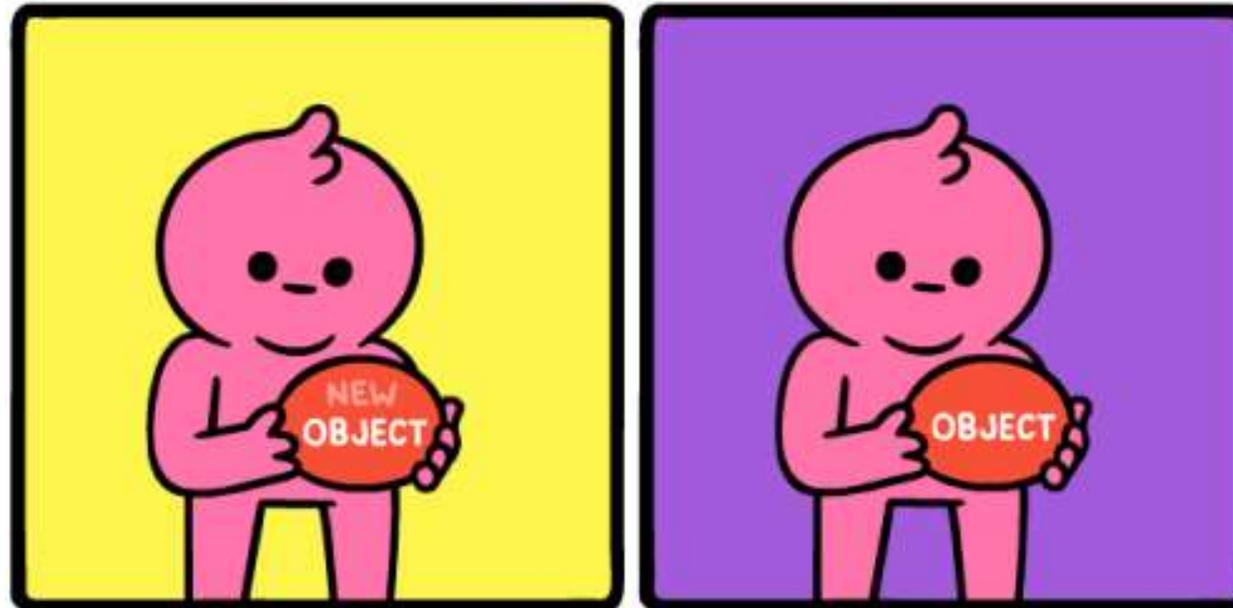
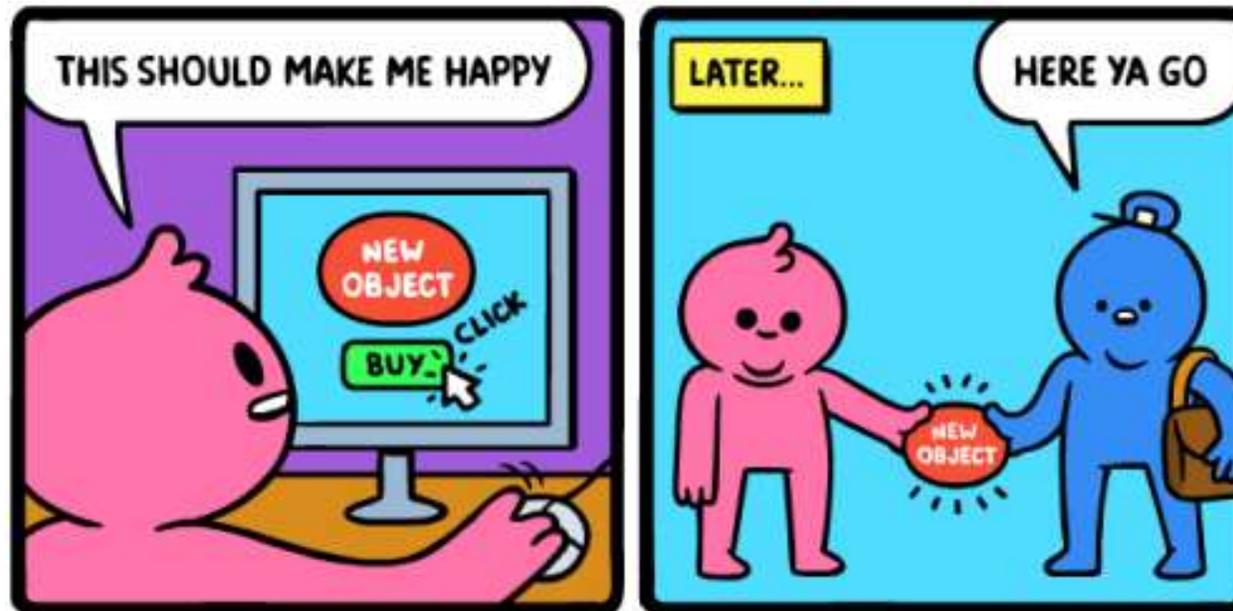
Robert Haist (CISO) @ TeamViewer

Let's

Talk

About

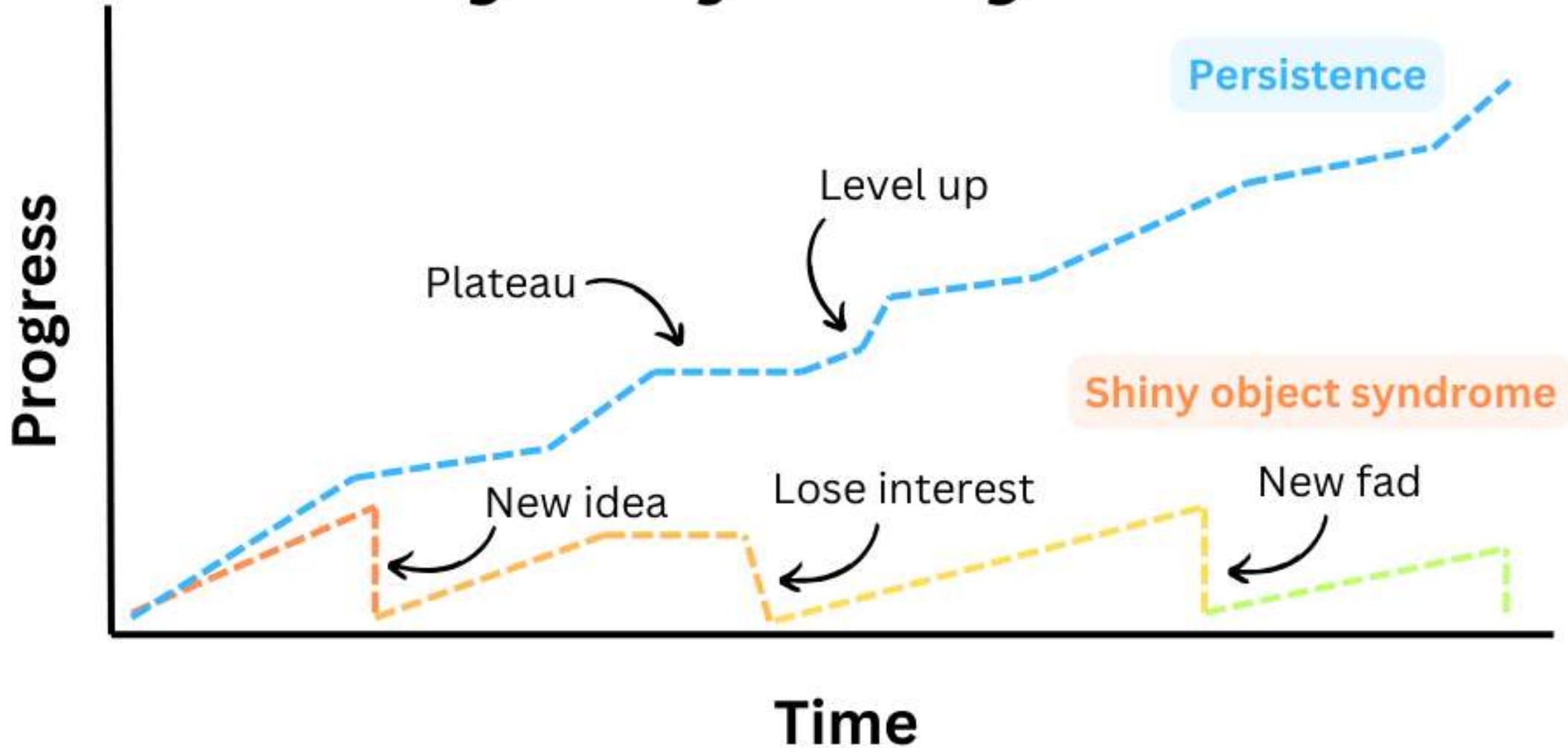
G.A.S.



THIS COMIC MADE POSSIBLE THANKS TO HARTESIC

@MrLovenstein • MRLOVENSTEIN.COM

Shiny Object Syndrome



Die ältesten Probleme unserer Branche

Dauerbrenner der IT-Sicherheit

- Ungepatchte Systeme
- **Schwache Passwörter**
- Fehlende Netzsegmentierung

Warum bestehen sie noch immer?

- **Vernachlässigung grundlegender Aufgaben**
- Fokus auf neue Technologien statt auf Basisarbeit
- **Wenig echte Lösungen sondern eher bessere Verwaltung der Probleme**

Die Herausforderung bei der Grundlagenarbeit

Langweilig und eintönig?

- Wiederholende Aufgaben wie Updates und Patches

Schwierig?

- Komplexität großer Netzwerke
- Widerstand gegen Veränderungen im Unternehmen („Gewohnheitsprinzip“)

Warum trotzdem wichtig?

- Fundament für alle Sicherheitsmaßnahmen
- Verhindert viele bekannte Angriffe (Pareto)

Back to Basics (Die Magischen Drei)



Multi-Faktor Authentication

- Single Sign On (SSO)
- Conditional Access
- Zero-Trust Access

FIDO2 ist dein Freund



Backups

- Niemand braucht Backups – Alle brauchen Restore
- Nicht getestetes Restore hat **Potential für unangenehme Überraschungen**
- Backup is nicht nur Daten sondern auch **“wie bekomme ich das von Null wieder ans Laufen” (BCM)**



Patch Management

- Geschwindigkeit ist Alles
- Ein kaputter Server ist weniger schlimm als Ransomware
- **Überprüfen ob Patches auch wirklich aufgespielt wurden**

Mehr Basics



Vorhandene Potentiale Nutzen

- Braucht man wirklich ein neues Tool oder setzt man vorhandenes einfach nicht sinnvoll ein
- Wirklich jede Neubeschaffung kritisch hinterfragen

Gedankenexperiment:

Wenn ich nur noch 50% der Tools haben könnte – welche würde ich behalten und warum



(Ganzjahres-) **Frühjahrsputz**

- Alle Accounts, Tokens, Service Accounts etc. die 90 Tage nicht benutzt wurden sperren
 - Nach nochmal 30 Tagen löschen
 - Dasselbe für Cloud Ressourcen
- Spart zudem Geld
- Was nicht da ist kann nicht gehackt werden



Awareness

- Faktor Mensch
- A Fool with a Tool is still a Fool
- **Gamification und Wertschätzung von Mitarbeit am Sicherheitsprogramm sorgen für nachhaltige Erfolge**

Nutzt 80% eurer Zeit und
Ressourcen für Grundlagenarbeit*

... und das Netzwerk wird langsam aber sicher sicher

* <https://www.cisa.gov/resources-tools/resources/cisa-cyber-essentials-starter-kit>

Thank
You

Robert Haist
Chief Information Security Officer

Robert.Haist@teamviewer.com