IoT = Internet of Threats ?

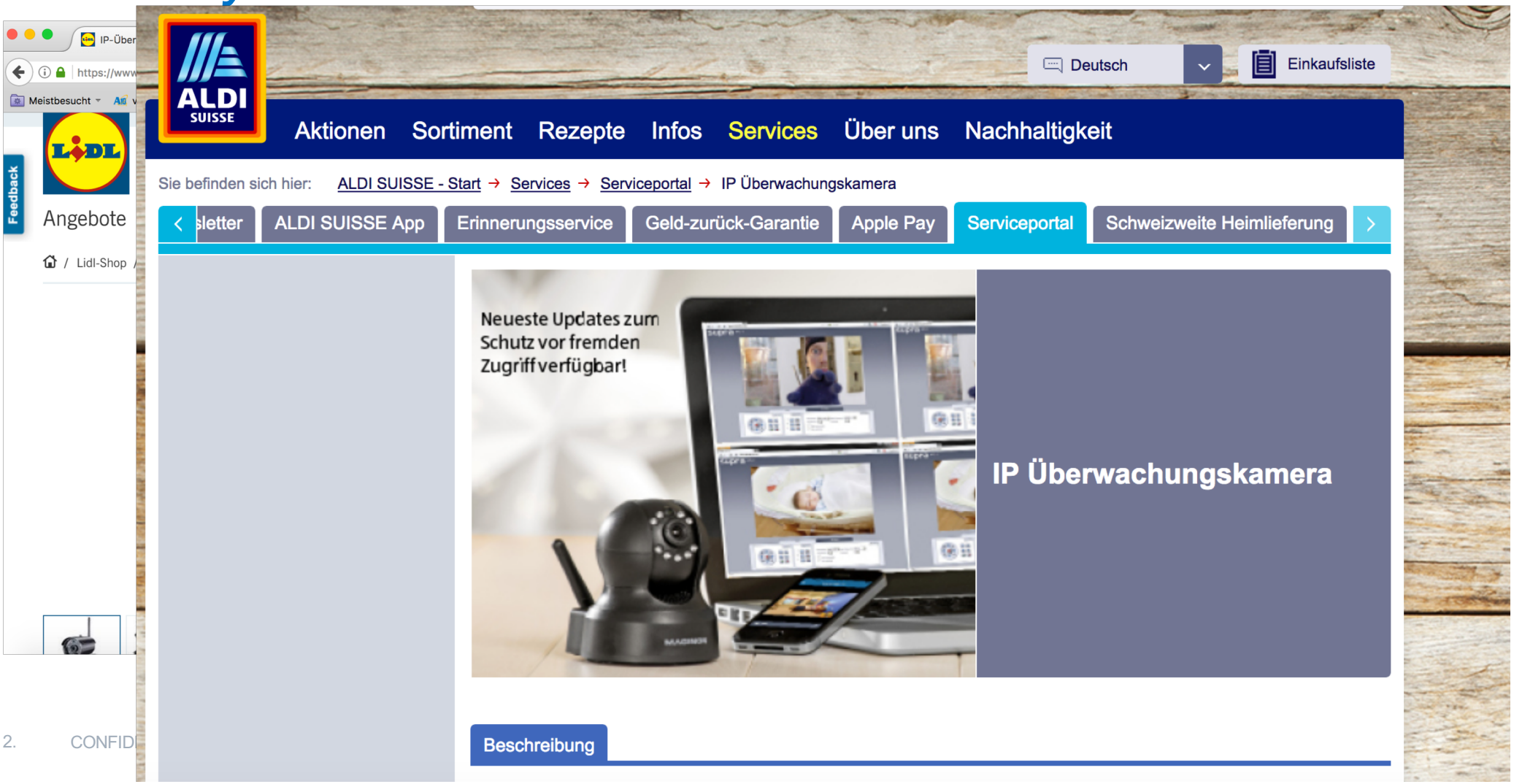
Heiko Frank

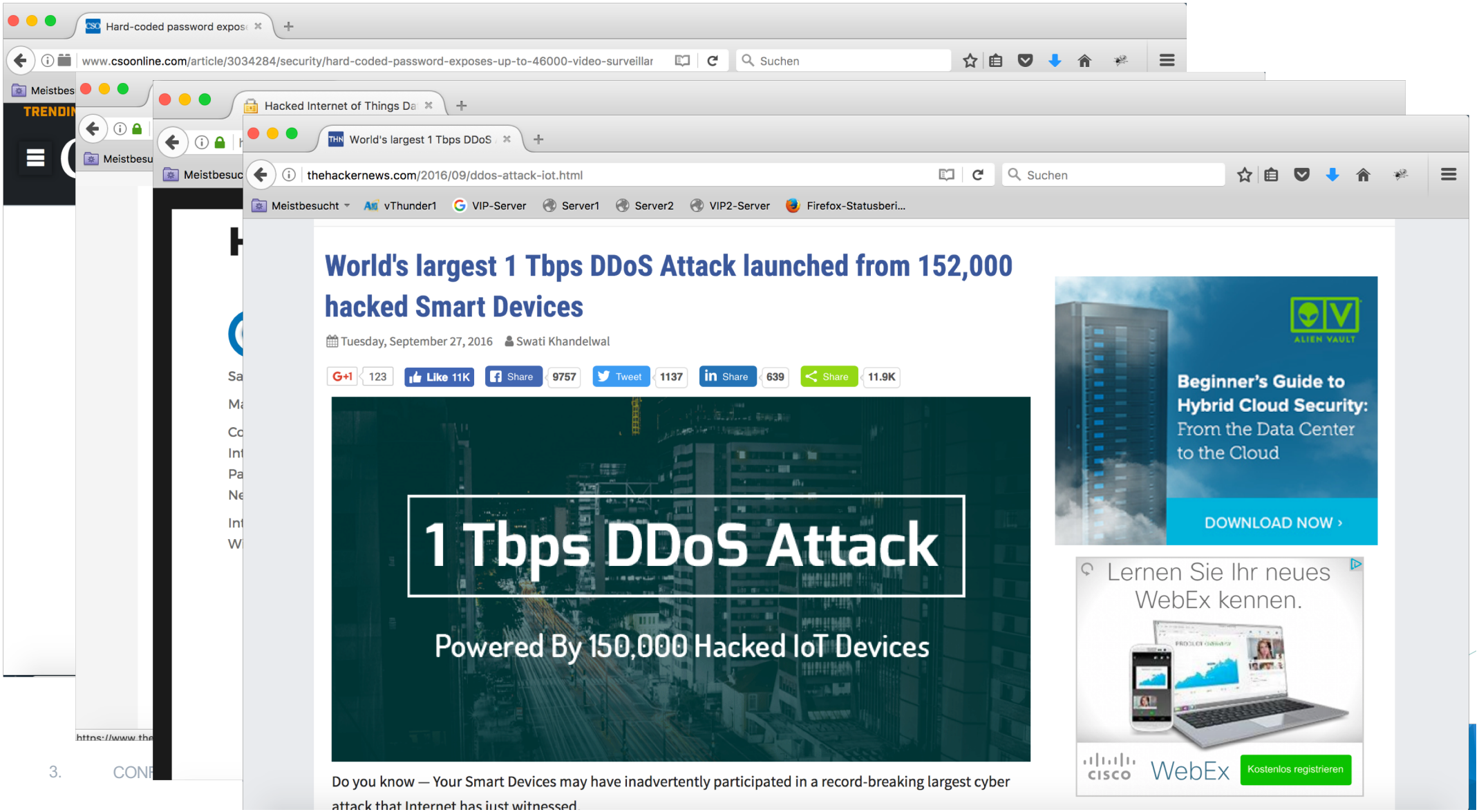
Principal System Engineer

Automation for Secure Applications

CONFIDENTIAL | DO NOT DISTRIBUTE

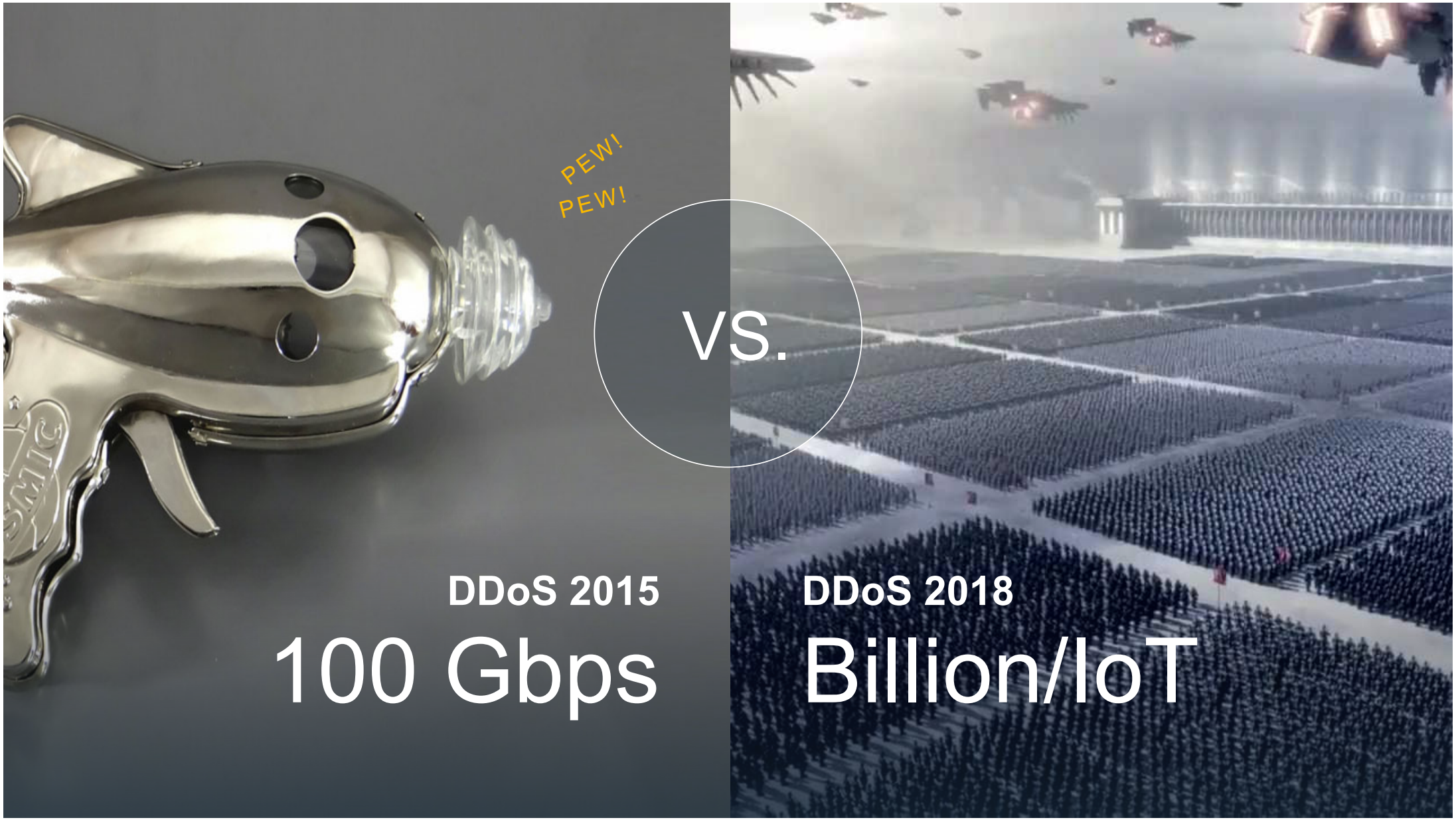
Saturday for Breakfast




Hard-coded password expos
www.csoonline.com/article/3034284/security/hard-coded-password-exposes-up-to-46000-video-surveillar
Suchen
Hacked Internet of Things Da
World's largest 1 Tbps DDoS
thehackernews.com/2016/09/ddos-attack-iot.html
Meistbesucht
vThunder1
VIP-Server
Server1
Server2
VIP2-Server
Firefox-Statusberi...
World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices
Tuesday, September 27, 2016
Swati Khandelwal
G+1 123
Like 11K
Share 9757
Tweet 1137
Share 639
Share 11.9K
1 Tbps DDoS Attack
Powered By 150,000 Hacked IoT Devices
Do you know — Your Smart Devices may have inadvertently participated in a record-breaking largest cyber attack that Internet has just witnessed
ALIEN VAULT
Beginner's Guide to Hybrid Cloud Security: From the Data Center to the Cloud
DOWNLOAD NOW ›
Lernen Sie Ihr neues WebEx kennen.
cisco WebEx
Kostenlos registrieren

Here's How The CIA Allegedly
https://www.forbes.com/sites/thomasbrewster/2017/03/07/cia-wikileaks-samsung-smart-tv-hack-security/#
Suchen
Meistbesucht
CIA macht Samsung Smart T
www.appdated.de/2017/03/cia-macht-samsung-smart-tv-zu-wanzen/
Suchen
Meistbesucht
vThunder1
VIP-Server
Server1
Server2
VIP2-Server
Firefox-Statusberi...
Cookies erleichtern die Bereitstellung unserer Dienste. Mit der Nutzung unserer Dienste erklären Sie sich damit einverstanden, dass wir Cookies verwenden. [mehr Informationen]
OK
Forbes
YOUR READING LIST
Here's Hov
Allegedly H
Samsung S
-- And Hov
Protect Yo
Workday V
The Innova
The Cataly
Driving Di
Transform
LISTEN N
Creative Br
And Badas
In STEM
Samsung SMART TV
CIA macht Samsung Smart TV zu Wanzen
BASTIAN EBERT am Mittwoch, 8. März 2017
dazu Allnet-Flat mit ...
mobilcom-debitel.de
freenetmobile
freeFlat ab 13,95 €
freeFLAT 2000: 2 GB LTE im D-Netz und Allnet-Flat*
freenetmobile.de
DAS NEUE IPHONE 7 UND 7 PLUS
Das neue iPhone 7 (plus) mit und ohne Vertrag im Überblick:

What is the problem?


PEW!
PEW!
VS.
DDoS 2015
100 Gbps
DDoS 2018
Billion/IoT

The World We Live In

DO YOU KNOW THIS MAN?

John Kelsey Gammell

"FBI convicted a Minnesota man for launching hundreds of DDoS attacks … former employers and business partners"

<- Paid: $652.87

vDOS

-> "30Gbps of Dedicated Bandwidth" and "Unlimited Boots."

Source: bleepingcomputer.com and Minnesota Star Tribune, Nov 6, 2017
https://www.bleepingcomputer.com/news/security/man-uses-ddos-for-hire-services-to-attack-former-employer-taunts-firm-via-email/
http://www.startribune.com/hacker-for-hire-cases-going-federal-in-minnesota/455624163/

BUSINESSES ATTACKED:

Washburn computer group

WELLS FARGO

JPMorganChase

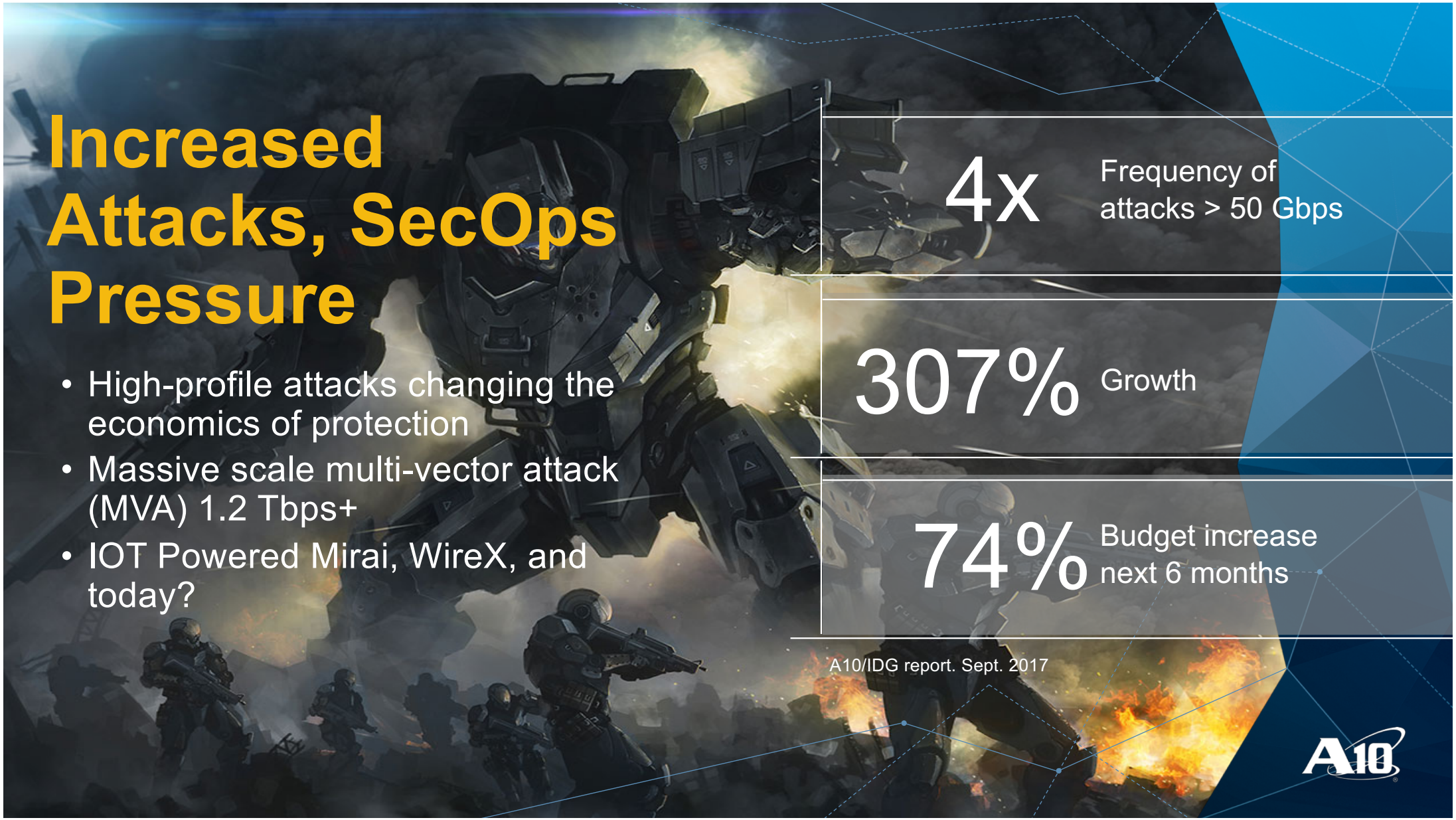
DAKOTA COUNTY TECHNICAL COLLEGE

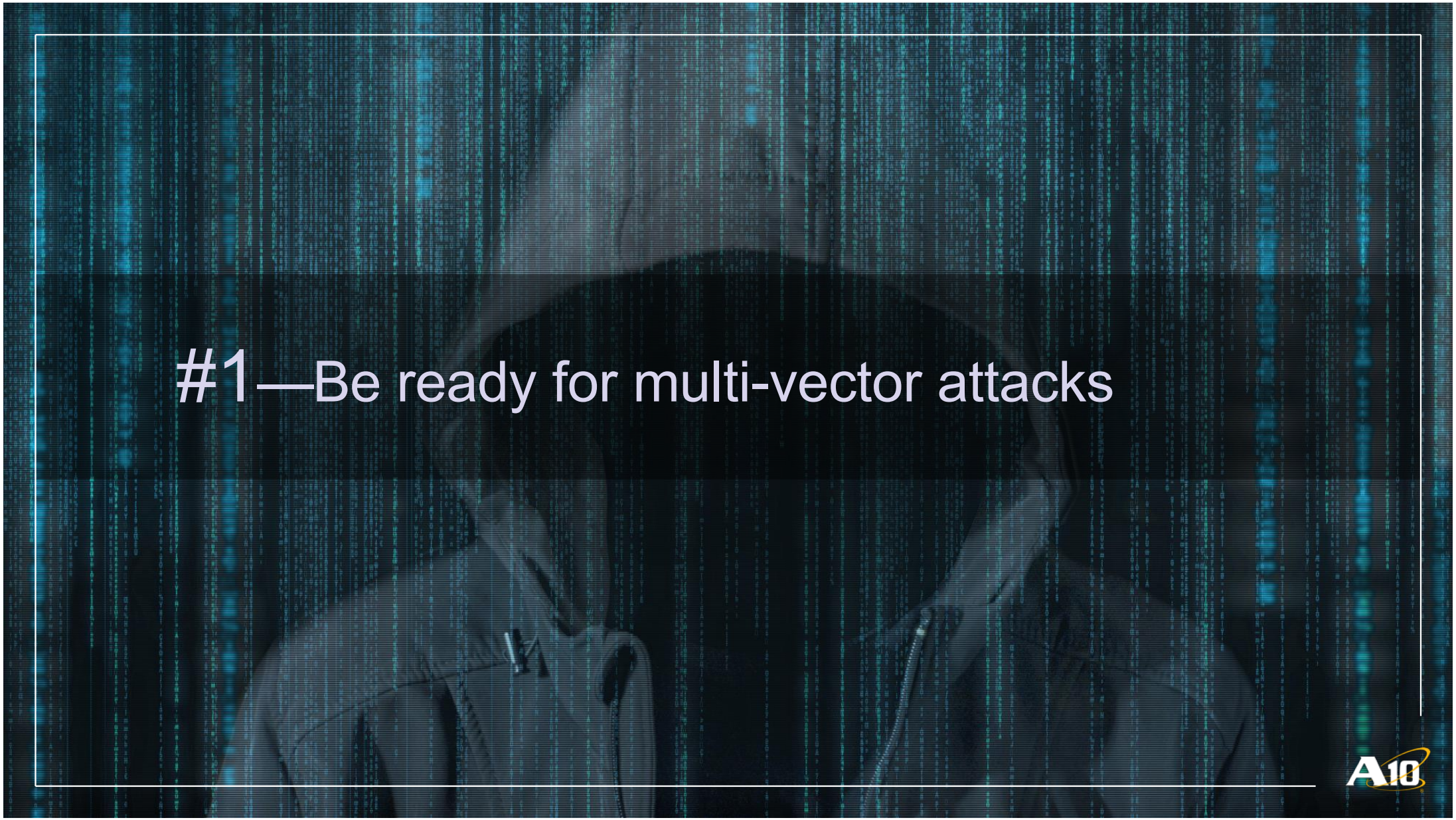
MINNESOTA JUDICIAL BRANCH

HENNEPIN COUNTY

sti electronics

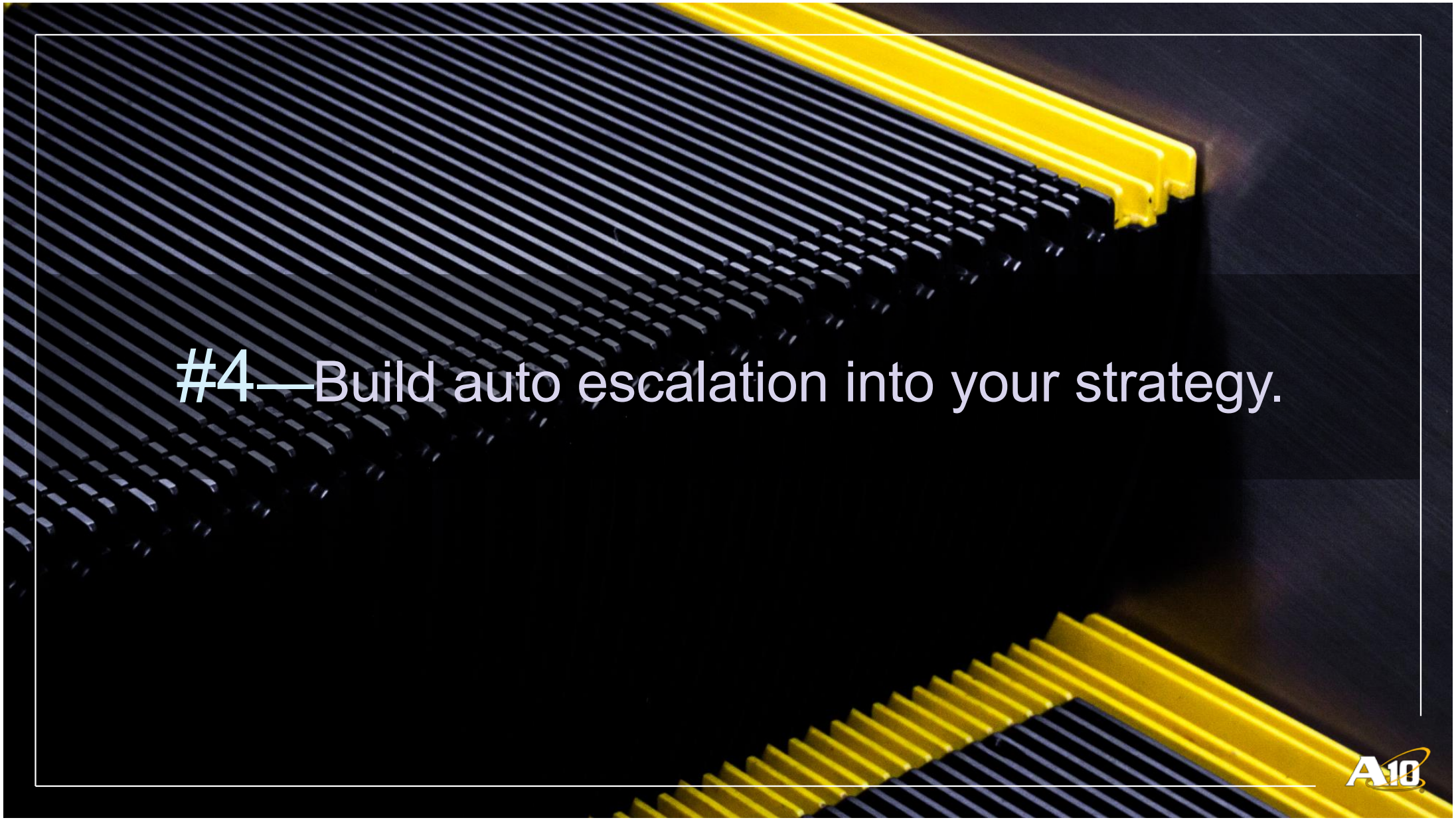
HKE


Increased Attacks, SecOps Pressure
• High-profile attacks changing the economics of protection
• Massive scale multi-vector attack (MVA) 1.2 Tbps+
• IOT Powered Mirai, WireX, and today?
4x
Frequency of attacks > 50 Gbps
307%
Growth
74%
Budget increase next 6 months
A10/IDG report. Sept. 2017
A10


#1—Be ready for multi-vector attacks

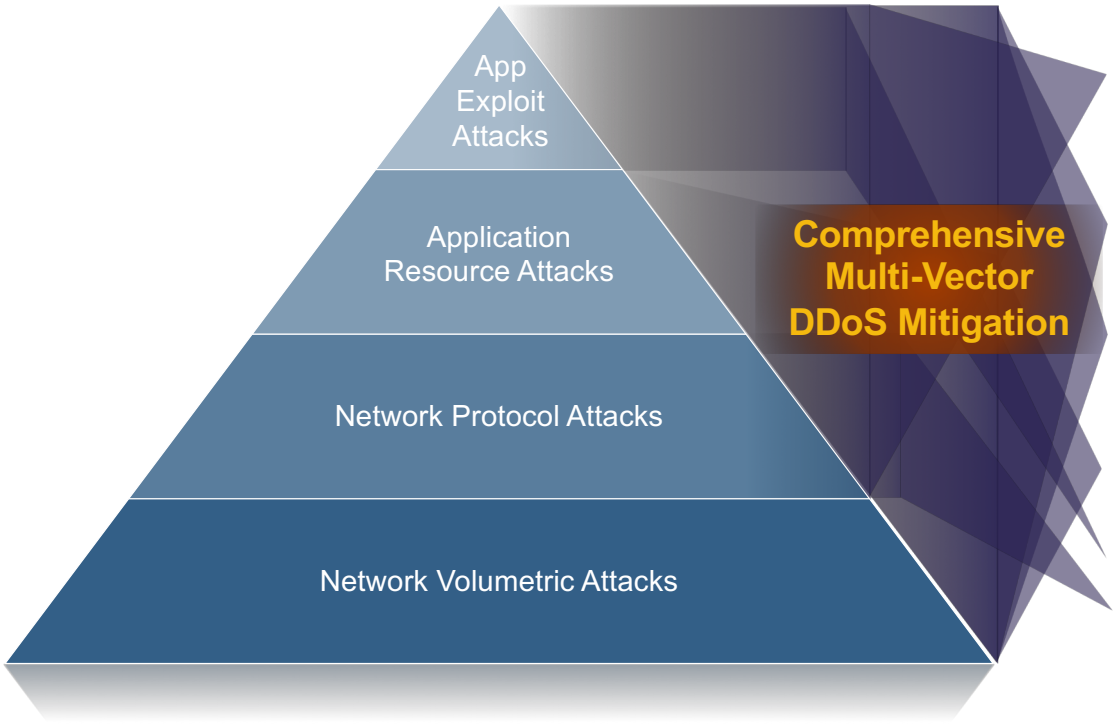
#2—Rate limiting isn’t enough.

#3—Leverage threat intelligence.


#4—Build auto escalation into your strategy.

#5—Get ready for scale.
A10

Mitigating DDoS Attacks Using Thunder TPS Series



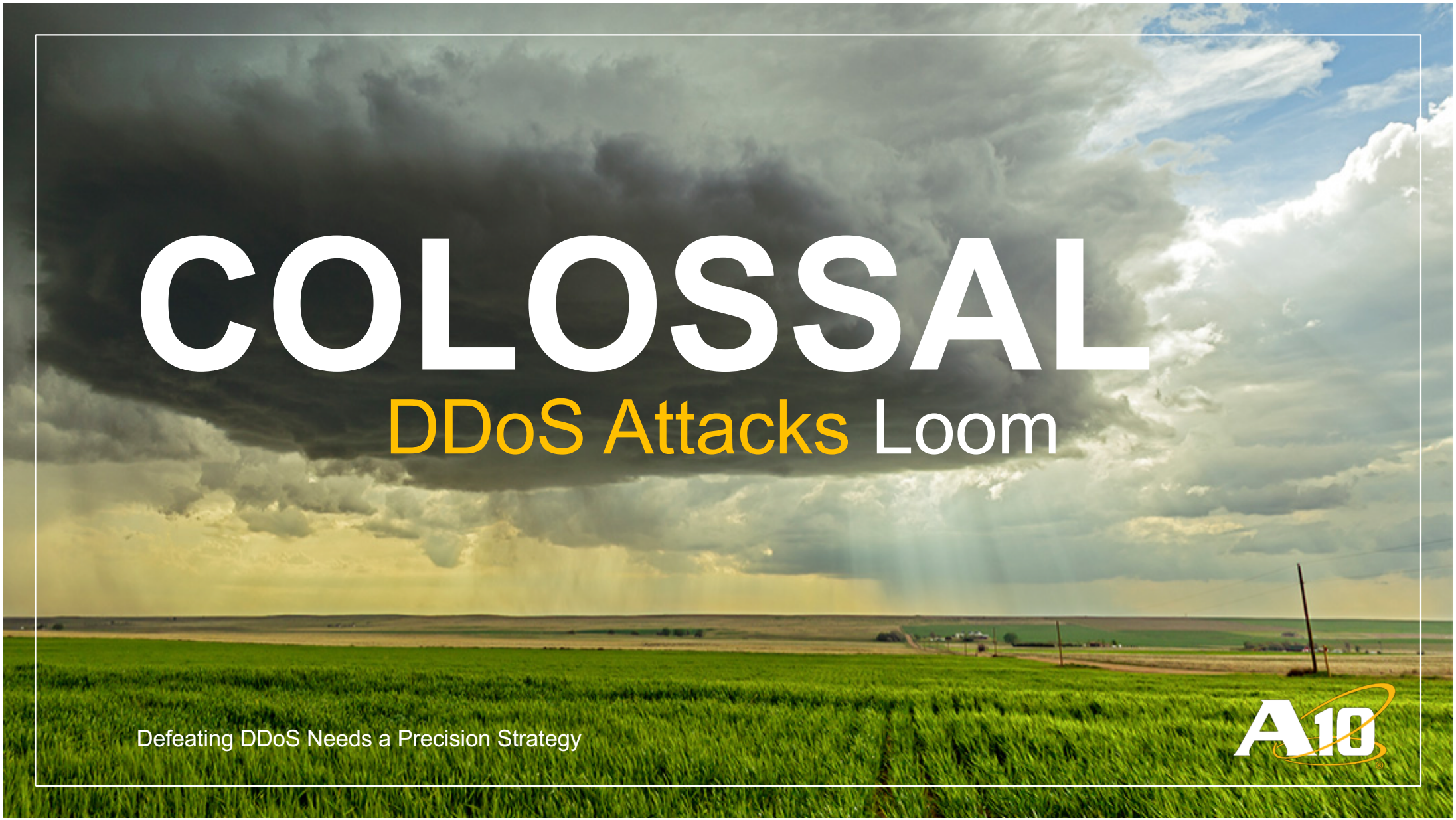
Behavioral Policies & Content Signatures
Thwart malicious behavior and surgically target content patterns

Challenge-Based Authentication
Identify malicious from legitimate clients

Black and White Lists
High-scale source-based admission control

Traffic Rate Control
High-granularity traffic rate enforcement

Packet/Request Anomaly Check
Validate incoming packets & requests


COLOSSAL
DDoS Attacks Loom
Defeating DDoS Needs a Precision Strategy
A10