
Xceptional / zadara
LIVE LINKEDIN Q&A
OCTOBER 12
Mastering IT & Cybersecurity Series: Ransomware & Zero Trust
Xceptional.com
CISCO
Partner

Session Structure

- Guest Introductions
- Trends
- Ransomware & Zero Trust
- Real World Examples, Situations
- Best Practices
- Wrap Up

Introductions

Host / Mark Dallmeier:

Industry Veteran, Researcher, CSO/CMO for Various Cyber Risk, MSSPs, MSPs.

Expert / Noam Shendar:

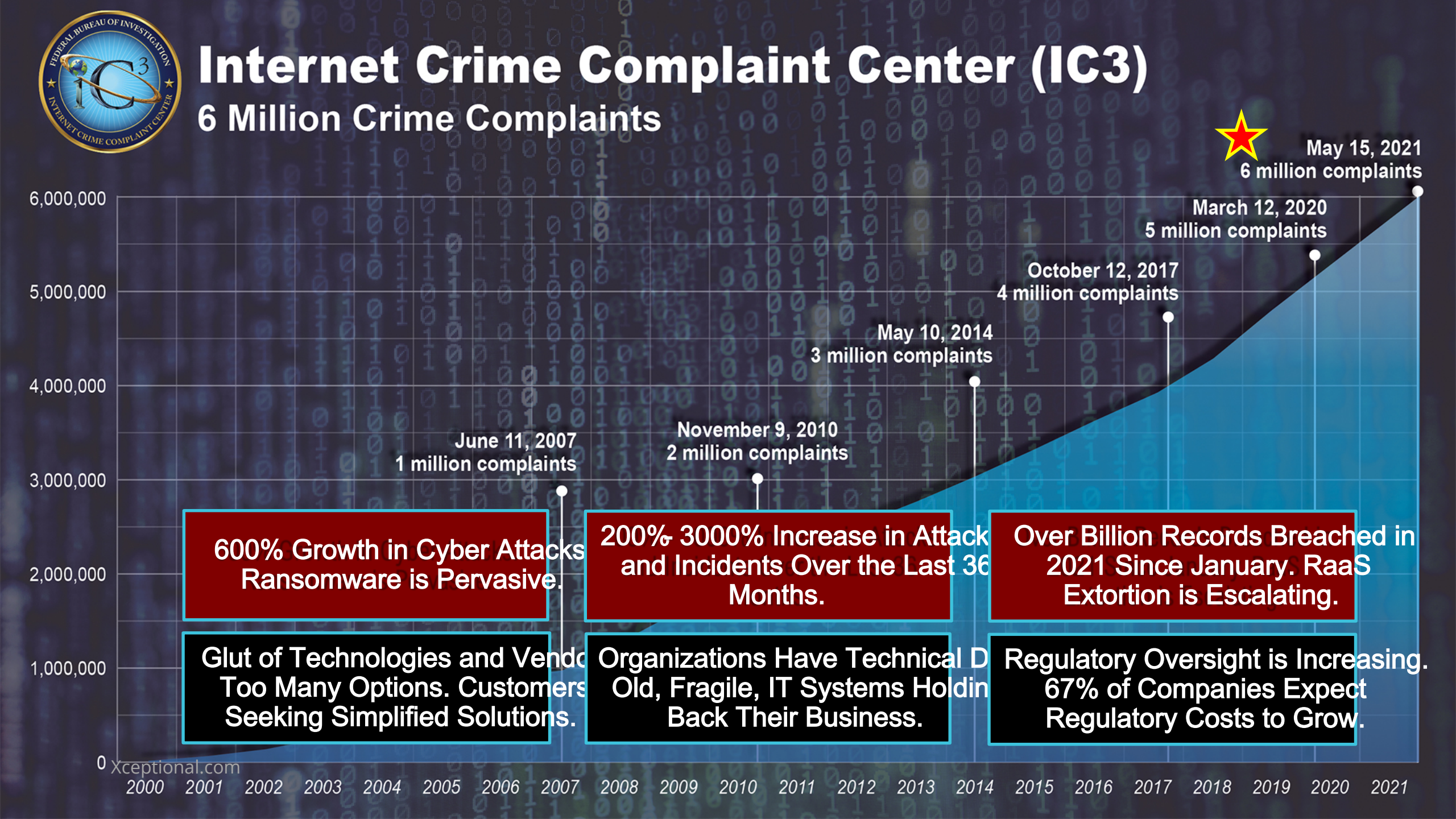
Industry Veteran, Executive VP WW Solution Architecture, Zadara

Expert / Don Maclean:

Industry Veteran, Researcher, Chief Cybersecurity Technologist, DLT

Internet Crime Complaint Center (IC3)

6 Million Crime Complaints



What Is Ransomware – Mark & Don

It is:

- a form of malware; software that is developed for nefarious or malicious purposes
- a family of malicious software with different variants, developed for different malicious purposes that has successfully impacted all industries across the globe
- a constantly changing, evolving code base that has been used to create (for hire) ransomware as a service offerings by hackers, cyber-criminals, nation states

It is not:

- slowing down, going away any time soon
- a single attack; it is often embedded and bundled together with other malicious code, virus, malware
- undefeated; it can be defended against

What Is Zero Trust – Don & Noam

It is:

- a philosophy or set of principles based on a realistic assumptions
- comprehensive, holistic approach to security
- a means to an end
- inclusive of many standard security practices & principles

It is not:

- a single product or technology
- limited to insider threat detection
- an end to itself

Problems that Zero Trust Solves

- Disappearing perimeter – no more "moat and castle"
- Growing attack surface
- Inevitable intrusions
- Long dwell times/Lateral movement
  - Bad actors stick around
  - They'll find everything eventually

Real World Examples, Situations

BUSINESS SITUATION	IT USE CASES	DIFFERENTIATION	
Growth, geographic expansion resiliency.	**Repatriation** Migrating Data between, Clouds, DCs and Co-Los	• No AWS / AZURE lock-in • Consistent performance • Cost savings & predictable costs	**Give Hypercloud Customers a choice w APIs**
Control or contain spending.	**CAPEX → OPEX at the Edge** How do we model Compute & Storage as a Service	• Select a partner and site that supports 100% pay as you go. • Up or down, by the hour • Full set off OpEx Services without committing to a Hypercloud	**Move Closer to OpEx**
Enhance employee and customer engagement, employee productivity.	**Edge & Latency** Needing cloud services closer to the source of data	• Lower latency, higher performance vs public cloud locations • Full suite of cloud services at the point of need • Your DC, Co-Location or Partner Data Centers	**Invoke the EDGE concepts**
Rapid response to market demands and needs.	**Utilize Local partnerships,** Knowledge and Infrastructure for Production, DR & Backup.	• Not simply being a NUMBER • Someone to call for support and questions • Completely connected to your success	**Work with a team you respect**
Architect IT systems and services to support business goals, objectives.	**Technology Refresh** Needing to keep IT resources current at a reduced costs	• Move to new technology when the timing is right • Accomplished 100% on the fly	**Keep IT fresh and new**

How Others Are Advancing Cyber Hygiene & Cyber Posture to Reduce Risk

Program Based on Principles
(*SOC-SIEM, Logging/Monitoring, Policies, Procedures, Resources)

People
(Security Education, Training, Awareness, Internet Usage, Phishing Simulations)

Patching, Scanning
(Vulnerability Management Program - Planned, Automated)

Passwords
(Unique Phrases w Special Characters, Vault)

- ✓ *Security Operations, SIEM, Scanning & Monitoring
- ✓ **Backups** (Full-Off Network)
- ✓ **Limit and Lock Down Administrative and System Access Control/Write**
- ✓ **Encryption** (At Rest, In Transit)
- ✓ **Limit, Block Network Access** (RDP, etc), email file extension delivery
- ✓ **End Point Detection & Response:** Modern Anti-Malware, Ransomware, Encryption on End Points
- ✓ **Updated BCDR Plans, Solutions** (Ransomware, Social Engineering)
- ✓ **IoT, IT Inventory, Assessment & Pen Testing**
- ✓ **Business Process Assessments**

- We ensure internal Security/IT departments and teams understand our short-mid-long-term business goals, objectives, priorities.
- We know where and how our Security/IT investments are adding value to the organization.
- We know how Security/IT teams are performing against their KPIs, metrics, expectations, outcomes.
- We know the current state of our Security/IT program and team maturity and effectiveness and how we use these capabilities to create business value and reduce or eliminate risk?
- We create dashboards, reports, or summaries, and communicate the value of Security/IT in terms that the business understand.

3-2-1-1-0: Data Protection

Veeam's '3-2-1-1-0' data protection best practice ensures data is completely protected from threats of all types — even ransomware. (object lock data immutability)

3 different copies of data

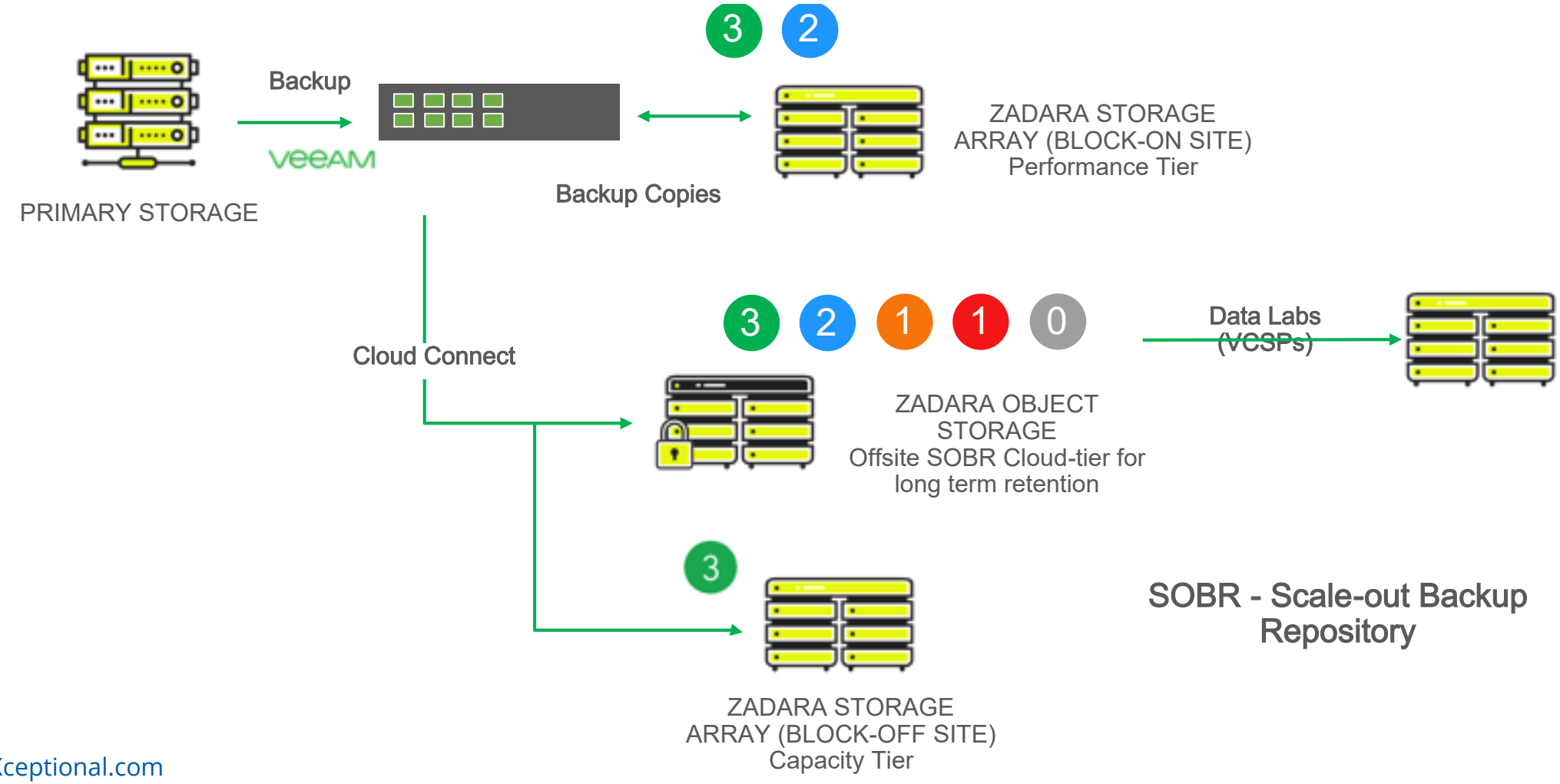
2 different media

1 of which is offsite

1 of which is immutable or air-gapped

0 Errors after backup recoverability verification

Back Up With Veeam: Ransomware Prevention



Cisco Zero Trust Technology Portfolio

Enabling Basic to Advanced Cyber Hygiene (Supports industry regulations)

Product	Capability	Basic 1	Intermediate 2	Good 3	Proactive 4	Advanced 5
ESA/WSA	Advanced threat protection capabilities to detect, block and remediate threats		■	■	■	■
Umbrella	Advanced defense and intelligence against threats	■	■	■	■	■
Duo	Establish user trust w/multi-factor auth, SSO for SaaS and device visibility	■	■	■	■	■
Cyber Vision	Threat detection/intelligence for cyber threats in the industrial networks		■	■	■	■
AnyConnect	Remote access to network with visibility and posture compliance via agent	■	■	■	■	■
SDA/ISE/TrustSec	Wired, wireless, VPN access policy with network segmentation	■	■	■	■	■
Tetration	Threat detection/intelligence for threats in the private/hybrid clouds	■	■	■	■	■
AMP/Threat Grid	Threat detection/intelligence with host visibility and remediation		■	■	■	■
Stealthwatch	Threat detection with internal network and cloud visibility via flow sensors		■	■	■	■
Threat Response	Threat visibility and rapid containment with intel-driven incident response		■	■	■	■
Firepower	Network access, segmentation and threat detection with in-line insertions	■	■	■	■	■

QA, Wrap Up & Next Steps

- **QA**
- **Key Takeaways from the Experts**
- **Offer: Complimentary Security Assessment**
  - Network vulnerability scanning
  - Technology review and evaluation
  - Controls review
  - Summary and recommendations report

info@xceptional.com


xceptional
zadara
Access more panels, webinars & research:
https://resources.xceptional.com/webinars
Contact Us Today!
cisco
Partner
xceptional.com | 858-225-6230