cisco Live!

#CiscoLive

The bridge to possible

Leveraging Machine Learning

To Better Prioritize XDR Incidents

Jerry Gamblin, Director Of Security Research
@JGamblin
PSOSEC-2012

Cisco Webex App

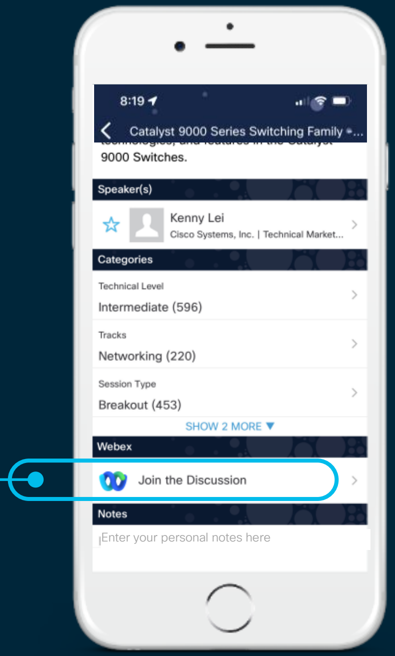
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#PSOSEC-2012

Agenda

- Ground Truth
- What is the Problem?
- How We Solved It For Vulnerabilities
- Can We Do It For XDR?
- What Is Next?

Ground Truth

The Goal of Security is to Prevent Breaches

The Goal of Security is to Limit Risk

The Goal of Security is to Ensure Integrity

What is the Problem?

We Are Data Rich…

- 65+ New CVEs released per day.
- 500,000 pieces of unique malware are detected every day.
- Average SIEM processes more than 25GB of data a day.

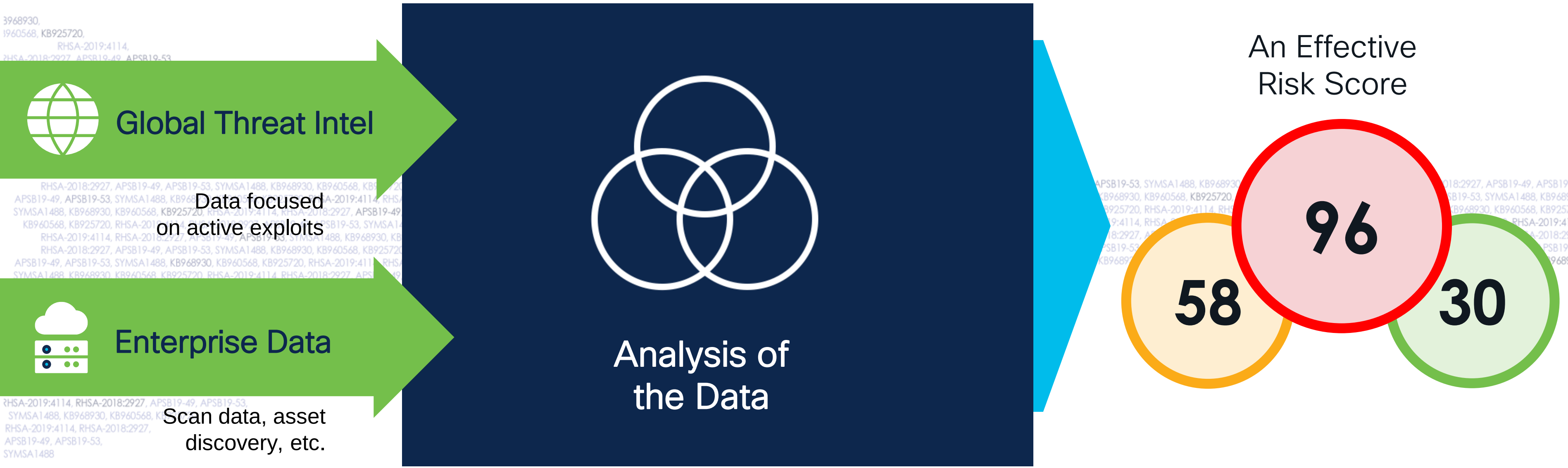
...but signal poor.

- Organizations can only remediate 15% of open vulnerabilities a month.
- Assets average 1.73 **actionable** alerts per year.
- Analysts have on average 7 minutes to triage an alert.

How Kenna Solved Risk Based Vulnerability Management

KENNA
Security
YEARS

The Risk-Based Approach



Global Threat Intel

Data focused on active exploits

Enterprise Data

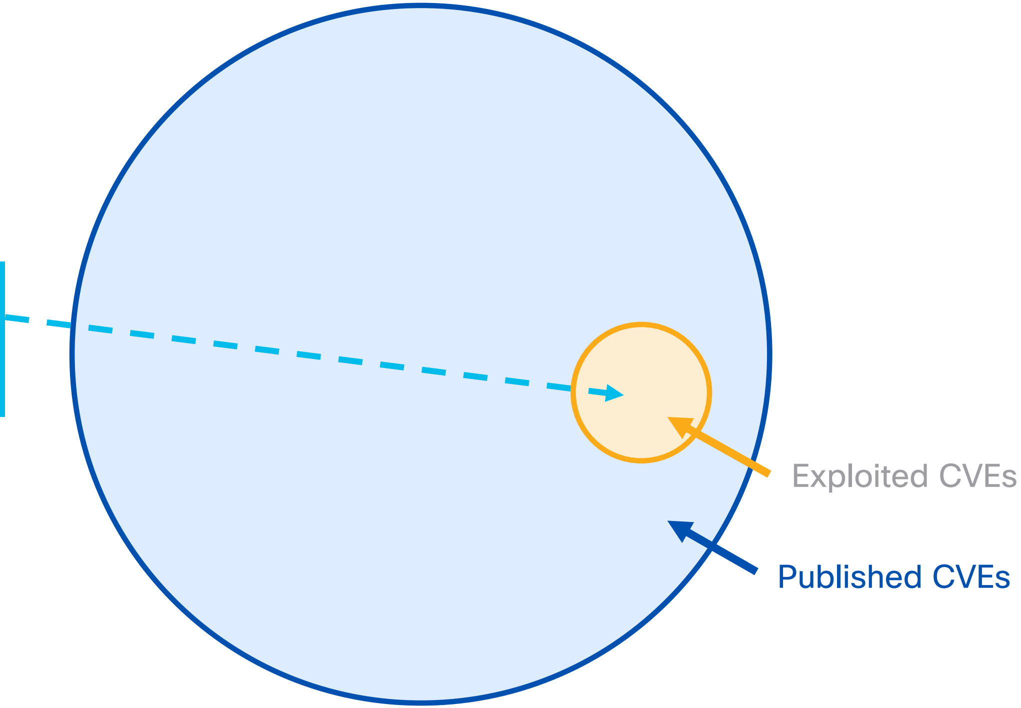
Scan data, asset discovery, etc.

Analysis of the Data

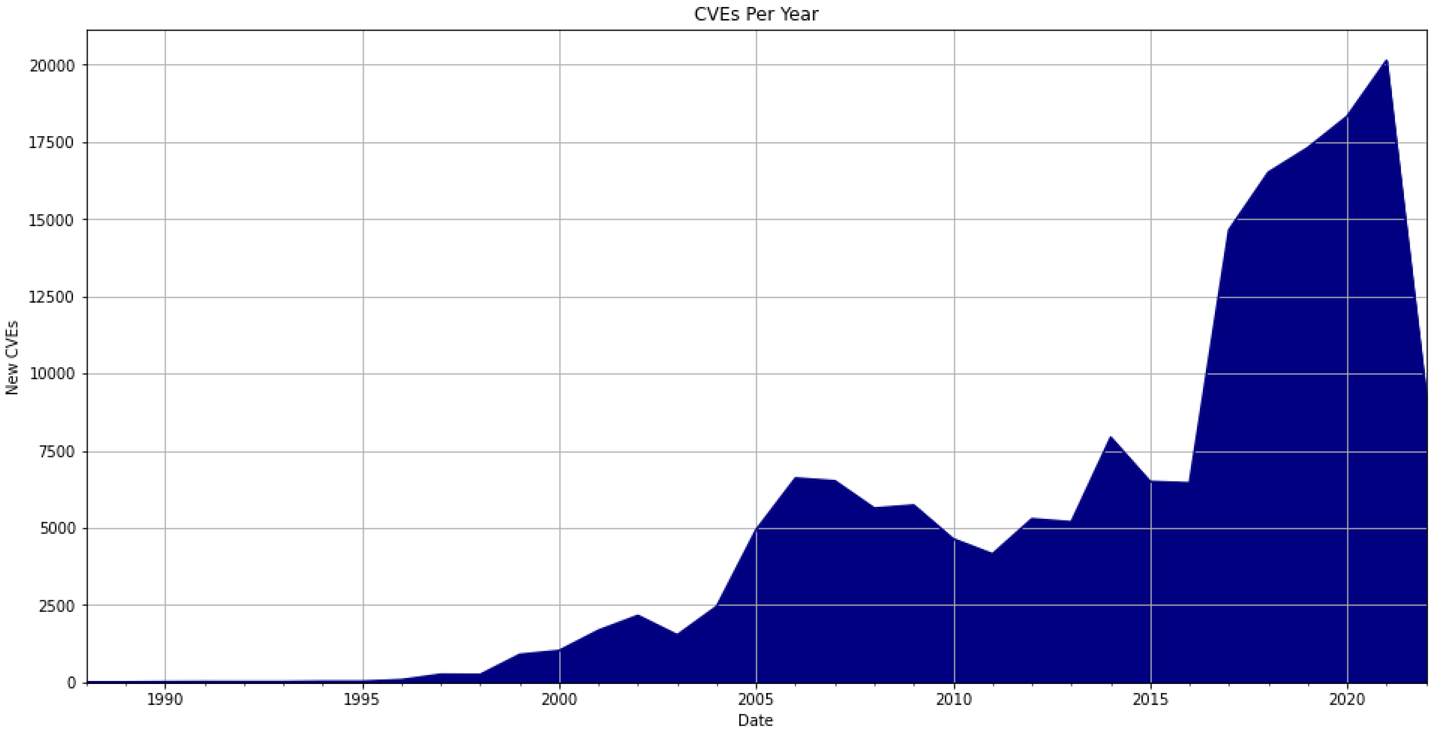
An Effective Risk Score

Remediation Goals

In a perfect world, we would focus our remediation efforts on the truly risky vulnerabilities.

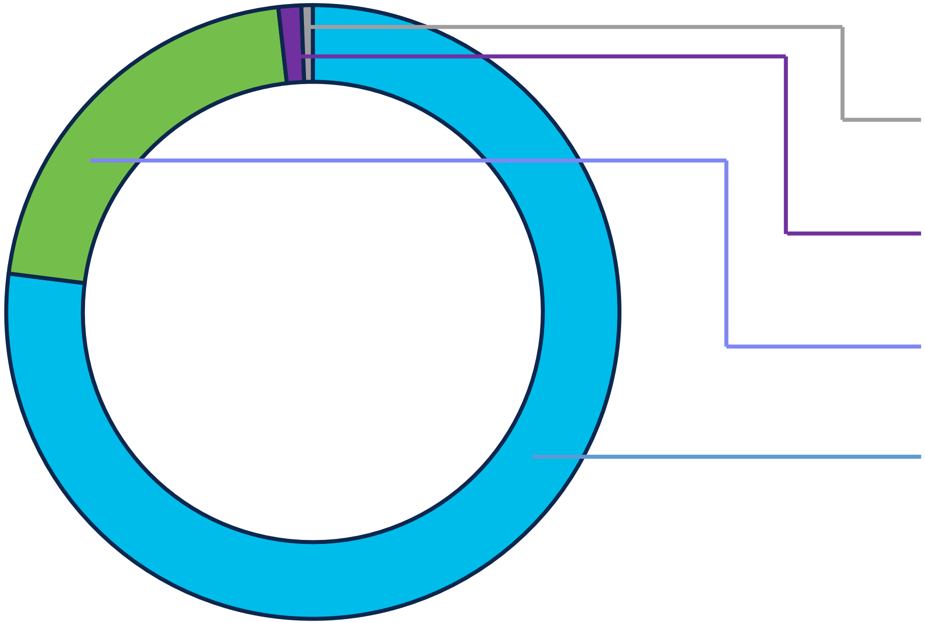


Let's Talk About CVE Data...



- CVEs from NVD: **176207**
- CVEs Published Per Day: **21.56**

Let's Talk About CVE Data...



0.6% of CVE’s just have executed exploits in the wild

1.2% of CVE’s have published and observed exploits

21.2% of CVE’s just have an exploit publicly released

77% of CVE’s have no published or observed exploit

Can we solve this for XDR too?

Let’s Do Some Math

2,087

Work Hours A Year (OPM)

1,565

Triage Hours (75%)

93,900

Triage Minutes per year

X = 93,900 Triage Minutes / 7 Triage Minute Per Event

13,414 Alerts

SIEM’s Are Not Helping

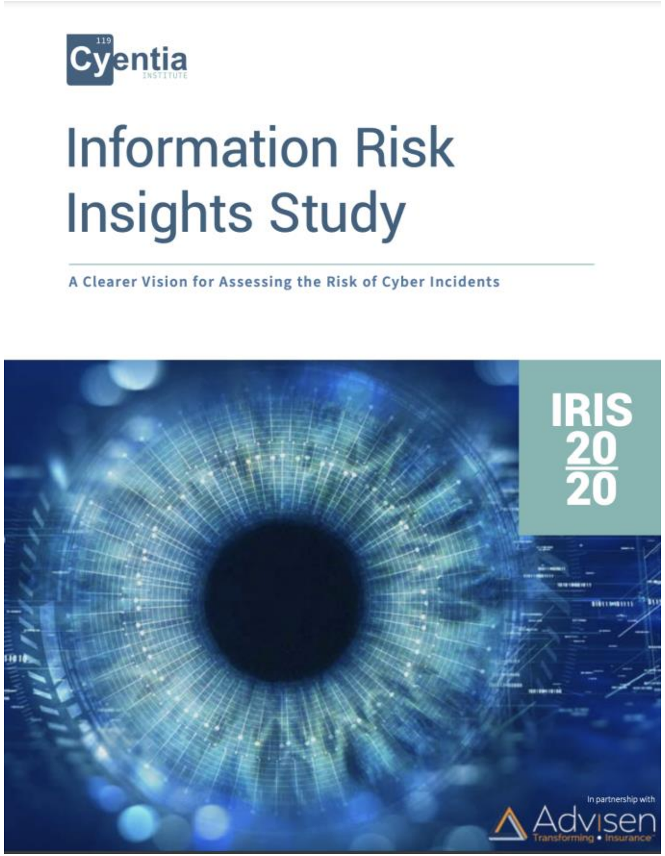
- 44% of orgs lacked staff to run a SIEM
- More Than 50% of organizations only investigate between 1 and 10 alerts per day
- 63% of respondents said they have trouble understanding report outputs by SIEM

XDR’s Are Not Either

- 38% of organizations have trouble filtering noisy alerts
- 37% have trouble accommodating security telemetry volume.
- 34% struggle to build a useful automation and alerting.

So, What Did We Do?

Information Risk Insights Study



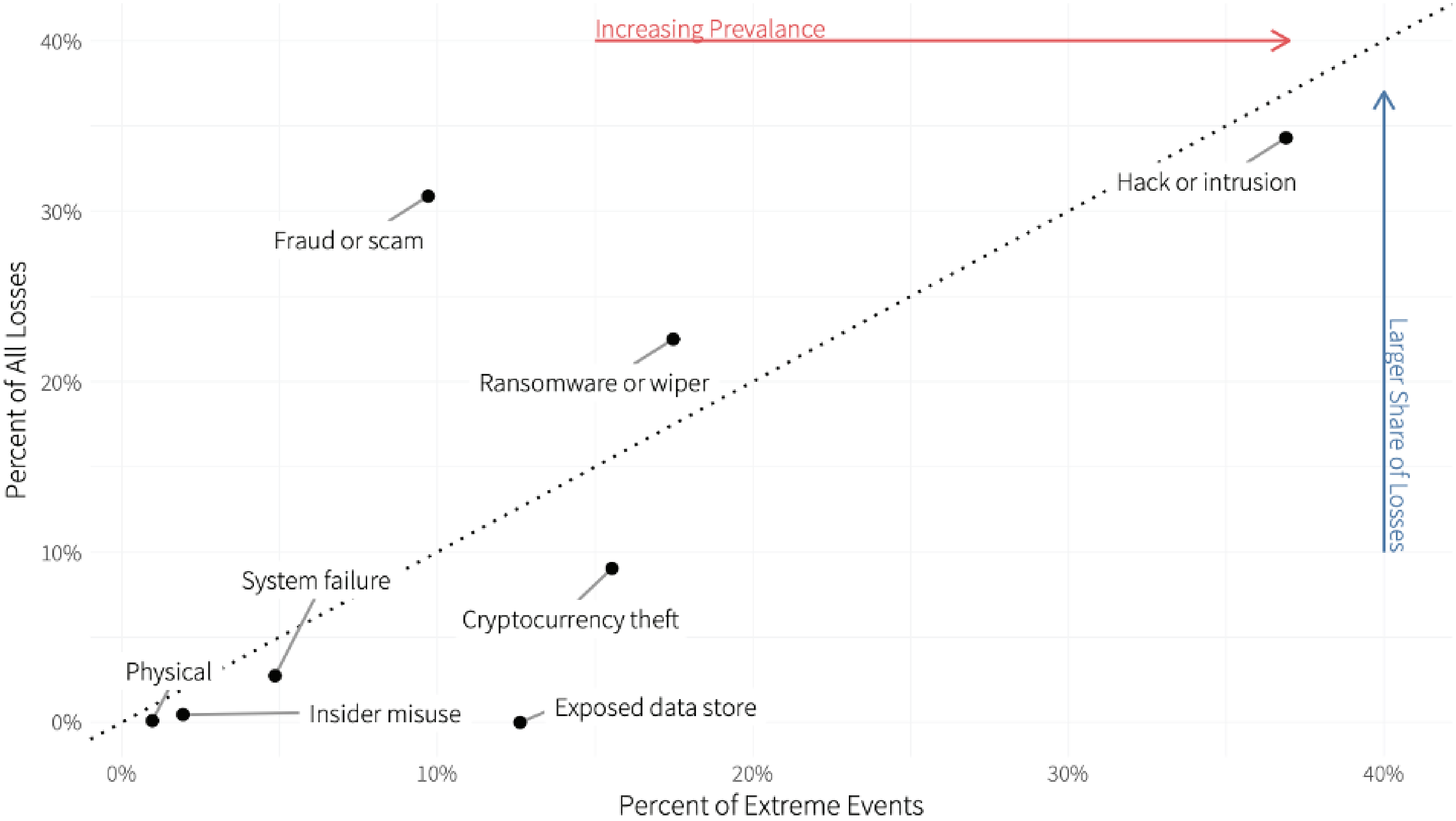
Cyentia INSTITUTE

Information Risk Insights Study

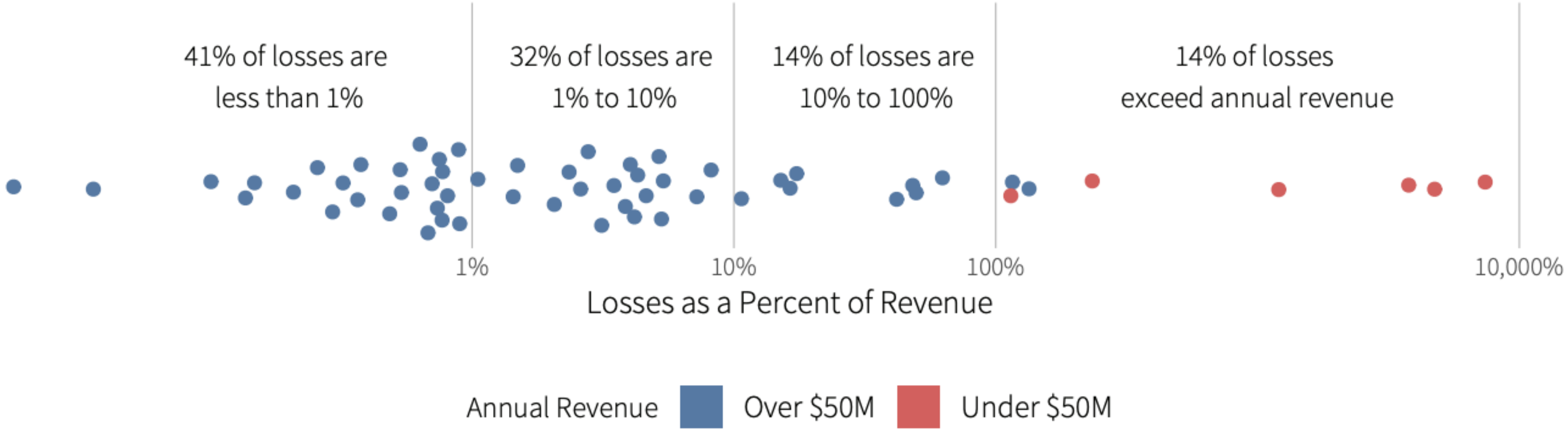
A Clearer Vision for Assessing the Risk of Cyber Incidents

IRIS 20 20

In partnership with Advisen Transforming • Insurance

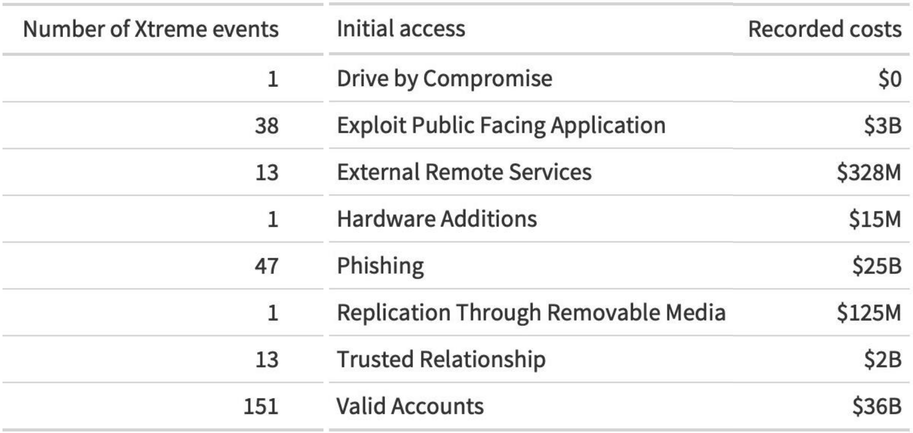

Increasing Prevalance
Larger Share of Losses
Percent of All Losses
40%
30%
20%
10%
0%
Fraud or scam
Hack or intrusion
Ransomware or wiper
System failure
Cryptocurrency theft
Physical
Insider misuse
Exposed data store
0%
10%
20%
30%
40%
Percent of Extreme Events

Cash Rules Everything Around Me



Where Is The Risk?

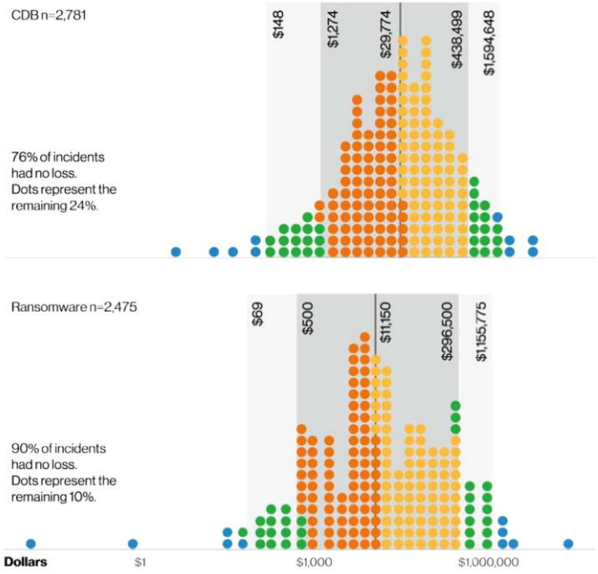
- Vulnerabilities are potential incidents.
  - We measured exploited vulnerabilities to see the probability of a potential incident turning into a real one.
- Incidents are potential losses.
  - We measure losses to see the probability of an incident mattering.



Number of Xtreme events	Initial access	Recorded costs
1	Drive by Compromise	$0
38	Exploit Public Facing Application	$3B
13	External Remote Services	$328M
1	Hardware Additions	$15M
47	Phishing	$25B
1	Replication Through Removable Media	$125M
13	Trusted Relationship	$2B
151	Valid Accounts	$36B

Most Incidents Don’t Matter

- **76%** of Computer Data Breach incidents had no loss.
  - **95%** were under $440k
- **90%** of Ransomware incidents had no loss.
  - **99%** were under $300k.



76% of incidents had no loss. Dots represent the remaining 24%.

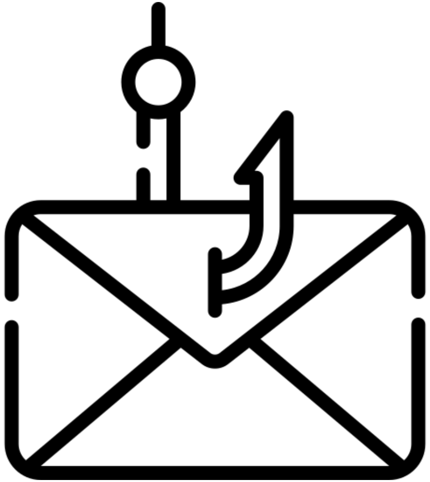
90% of incidents had no loss. Dots represent the remaining 10%.

Figure 40. Loss by incident type
Each dot represents 0.5% of incidents

Some Incidents Do Matter...

Process Injection

- T1055
- 5 events totaling **$985M** losses



Phishing

- T1566
- 47 Events Totaling **$25 Billion**

How Is Cisco Solving This?

7(s+4)+36
(s²+16s+25)
[20e - 13·e^-7t] u(t)

The Cisco Advantage

The Cisco approach to XDR

Integrated Solution

connecting multiple point solutions and data silos – Cisco and 3rd party

Undisputed Evidence

real-time threat intelligence focus on active threats, informed by Talos and Kenna, with unmatched data science

Rapid Response Actions

dramatically decrease MTTR and free up resources through automatic orchestration

Boundary-Free Scalability

enterprise-ready, and open ecosystem for multi-vendor environments

Effective Prioritization

focus on ***real risk*** and impact to enterprise

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

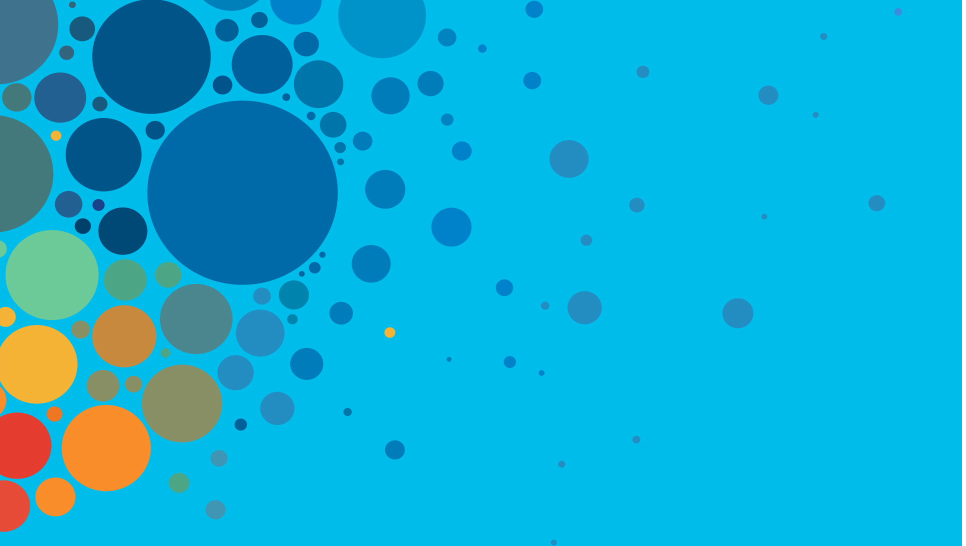
Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

cisco Live!

#CiscoLive