CSO Conference *& Awards*

Produced by CSO | IDC

Accelerating & Automating EASM

Leveraging AUTOMATION to make quick decisions about External Attack Surface Risks

intel

CSO Conference & Awards | intel

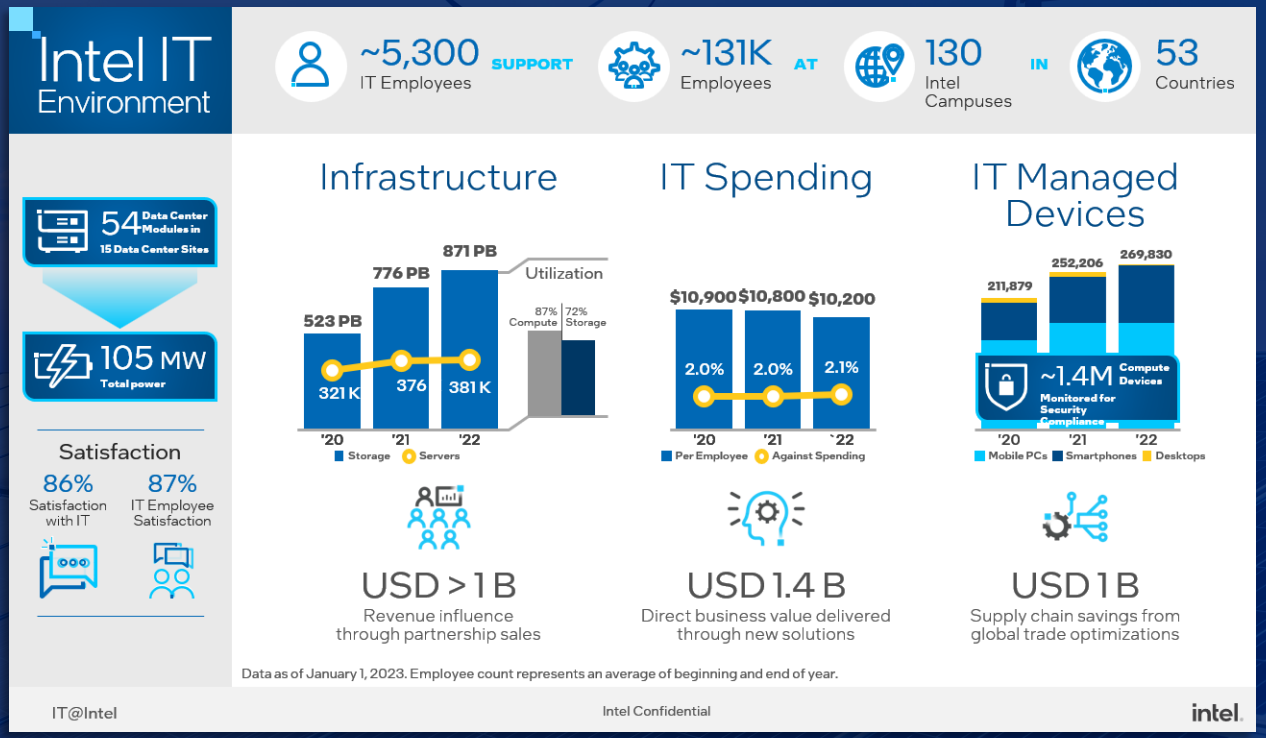
Produced by CSO | IDC

Introductions

Andy Ambrosia
Cyber Defense EASM SME

Alan Gonsalves
Cyber Defense Solution Group Owner

Tony Saint
Cyber Defense Director



The Problem

How to Drive & Keep Perimeter Risks at Goal - Real Time, Efficiently?

Mountains of Cyber Data

Apply Defense in Depth

Manage Multiple Controls

Informed, Risk-Based Decisions

Our Solution

Pivot from a vulnerability scanning centered approach to a comprehensive framework of data driven risk indicators

Cyber Intelligence

External Data & Discovery Sources

Assessed EASM Exposure

Internal Data Lake

Configured Risk Tolerance

Data Automation

Automated Dashboard

EASM RESIDUAL RISK : 8%			
6.0%	2.0%	5.1%	8.0%
10.2%	8.9%	2.9%	5.2%
3.2%	7.0%	1.7%	14.0%

Scope: Digital Attack Surface

32 Actionable Metrics: Owners, Goals & Escalation Workflows

Drive to Closure

Accountability

Automated Risk Response:

- *Owner Notifications*
- *Vulnerability Prioritization*
- *Incident & SLA Monitoring*
- *Remediation Tracking to Security Incident Closure*

Critical Success Factors

Foundation

- Cross IT and Business Group partnership on shared goals
- Leverage industry & technical solution partner best practices
- CISO & Executive “Tops Down” Sponsorship end-to-end

Automation

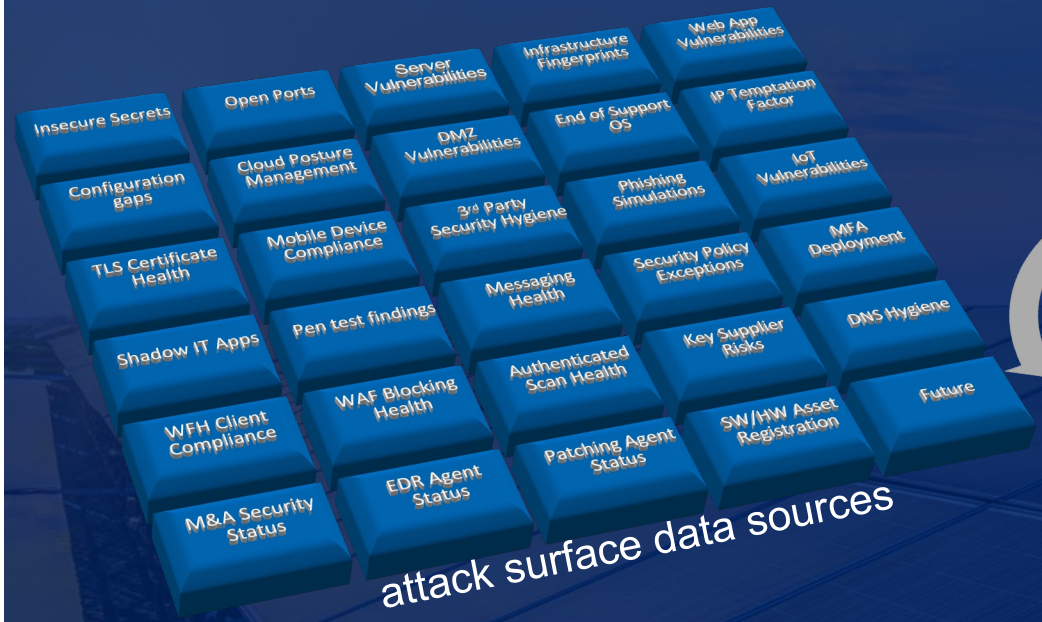
- Clear visibility into risks from all sections of the attack surface
- Clear indication when risk exceeds tolerance
- Subject matter experts aligned to each section of the attack surface
- Ability to expand breadth and depth at scale

Execution

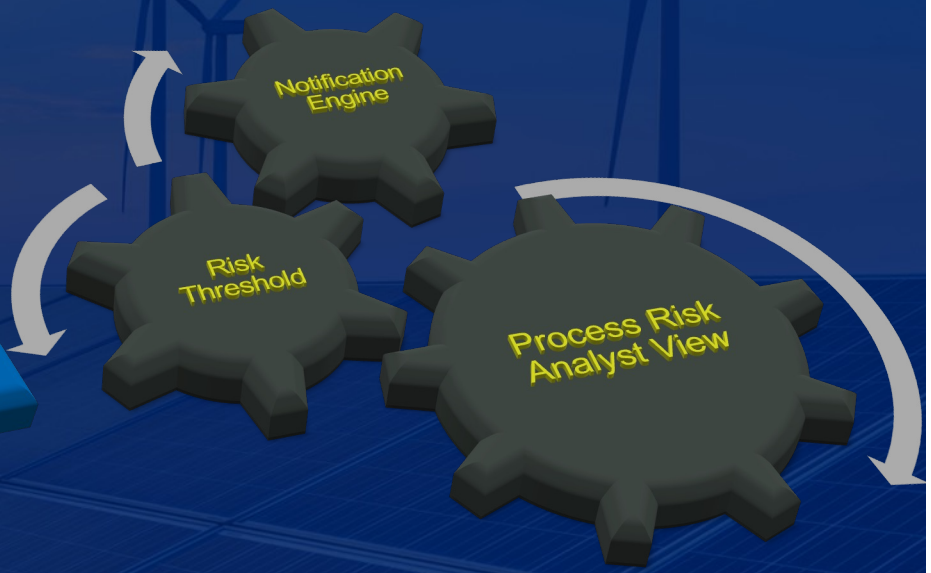
- Daily EASM Operations to remediate risks exceeding tolerance
- Ability to make rapid data-driven decisions about risk
- Iterative: Learn, Refine, Expand

EASM Framework

Risk Based Automation



attack surface data sources



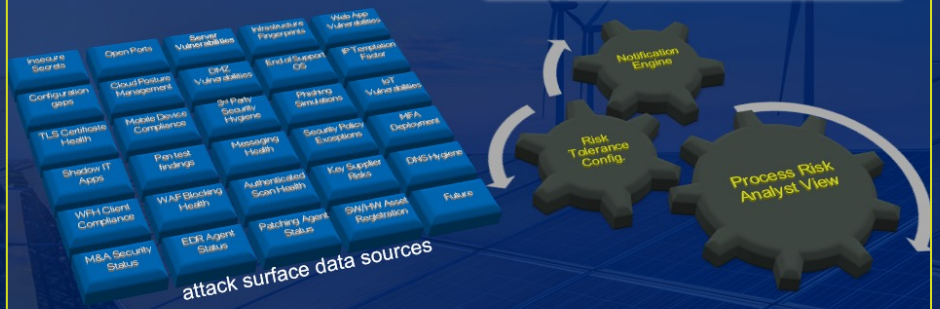
Data Driven Ops

Putting it all together

Workflow Engine

EASM Framework

Risk Based Automation



Automated Dashboard

EASM RESIDUAL RISK: 8%			
6.0%	2.0%	5.1%	8.0%
10.2%	8.9%	2.9%	5.2%
3.2%	7.0%	1.7%	14.0%

Scope: Digital Attack Surface

32 Actionable Metrics: Owners, Goals & Escalation Workflows

Problem	Solution	Impact
Leverage rich cyber data sources	Orchestrated cyber data feeds automation engine into EASM Dashboard.	EASM KPI Goals met or exceeded continuously
Gain a comprehensive picture of risk on the external attack surface	Daily operations that drives risk closure	Highly efficient real time understanding of EASM Risk
Efficiently Drive Perimeter Risks to Risk Tolerance & Sustain	Flexible to leverage growing cyber data sources	Risks resolved to prevent or mitigate exploitation

CSO Conference & Awards | intel

Produced by CSO | IDC