RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART1-R01**

Expect More: Realizing the True Impact of Your Intelligence Program

Stu Solomon

President
Recorded Future®

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The Bottom Line Up Front

- Why it's worthwhile to manage risk beyond audit compliance
  (hint: the accelerating convergence of the physical and cyber worlds)
- How intelligence informs strategic security priorities and reduces uncertainty
- Building scalable and consumable intelligence
- Why automation in intelligence is critical to creating measurable operational outcomes
- We need to expand the paradigm for the use cases of intelligence

Image Source: coscon.princeton.edu

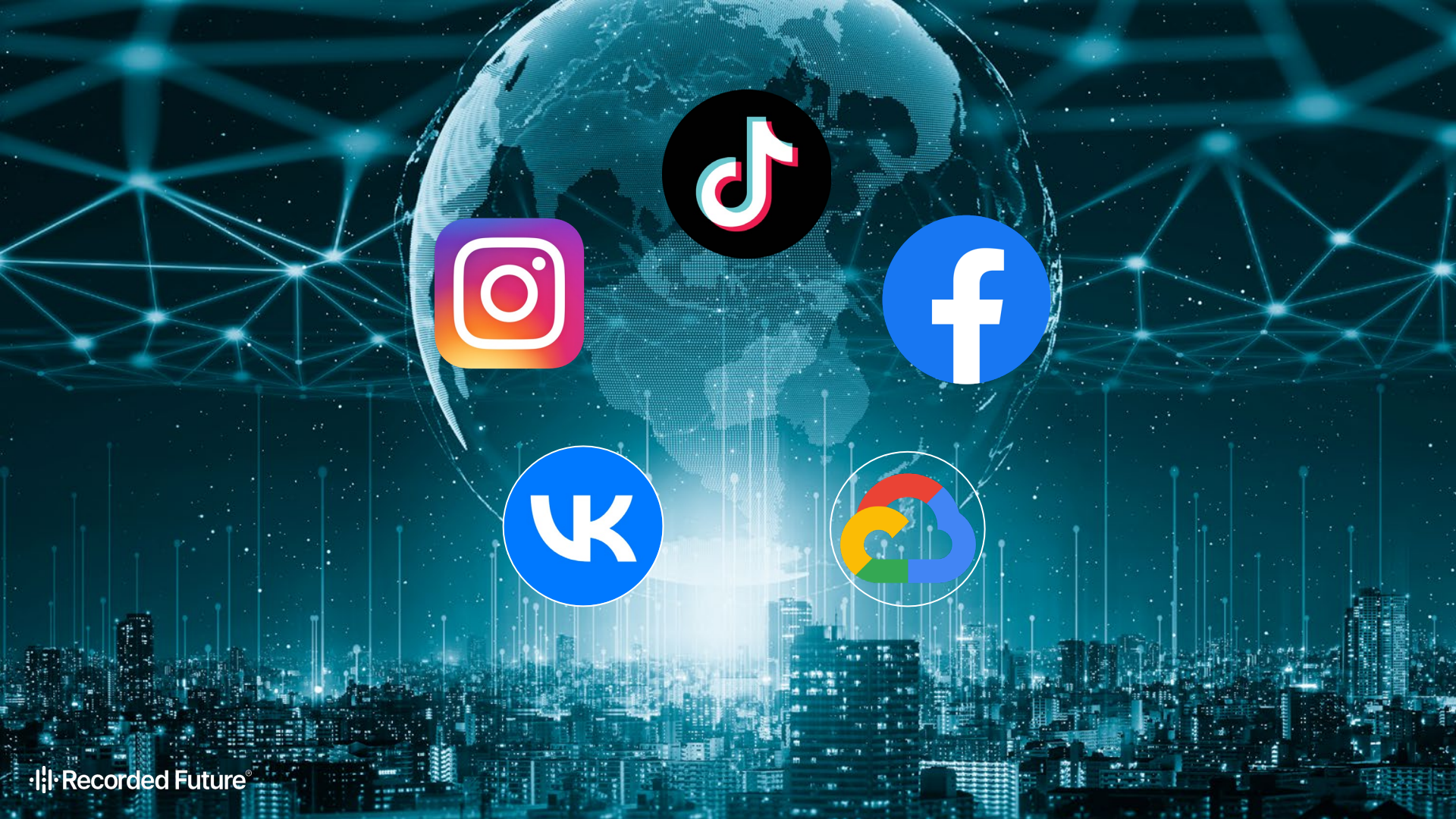

Everything Eventually Ends Up on The Internet
Where the world’s information, transactions, IP, and money resides and travels
Recorded Future®


Everything Eventually Ends Up on The Internet
Where cyber attacks are planned, executed, and profited from
Recorded Future®

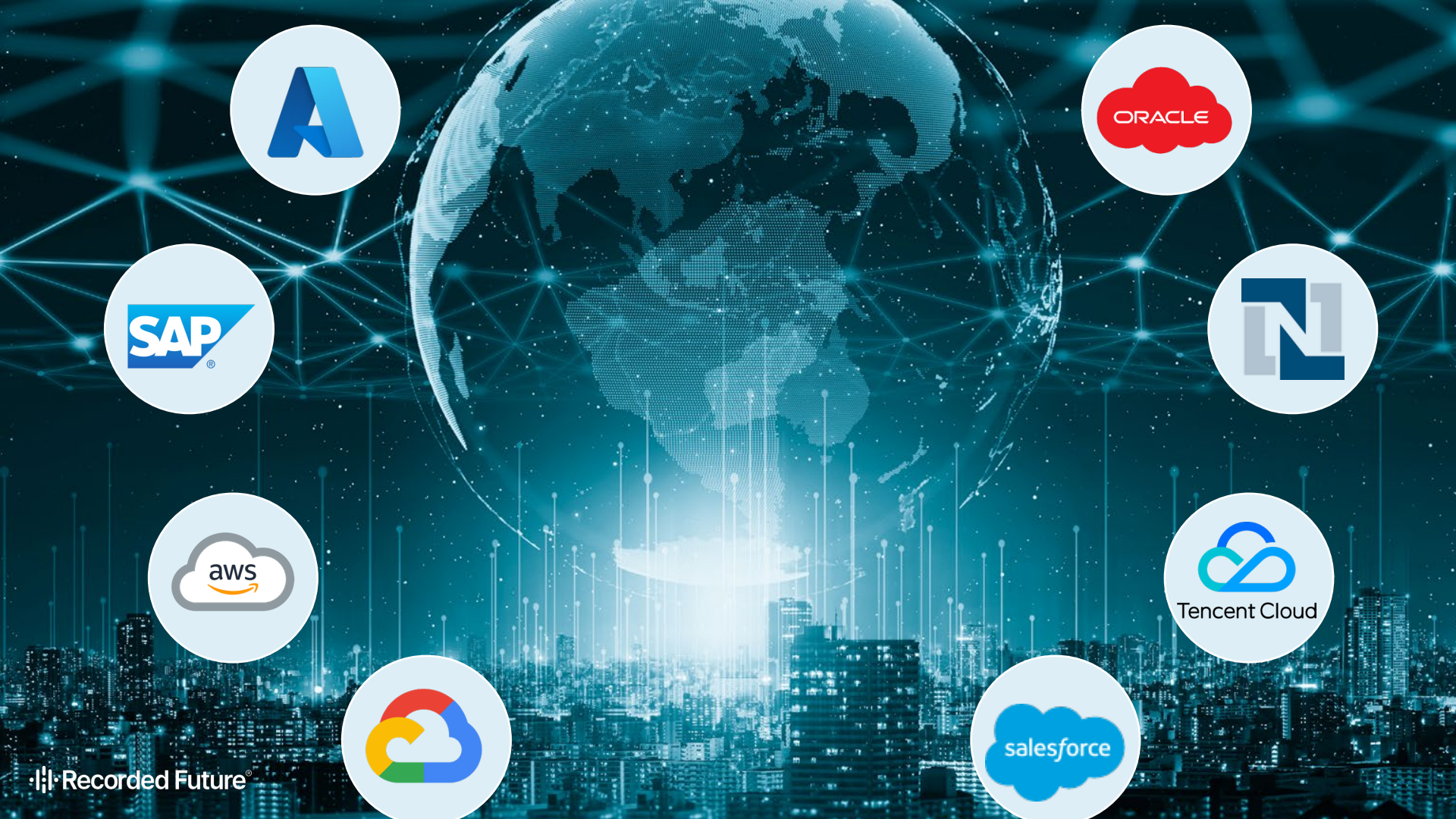
The Opportunity And The Challenge

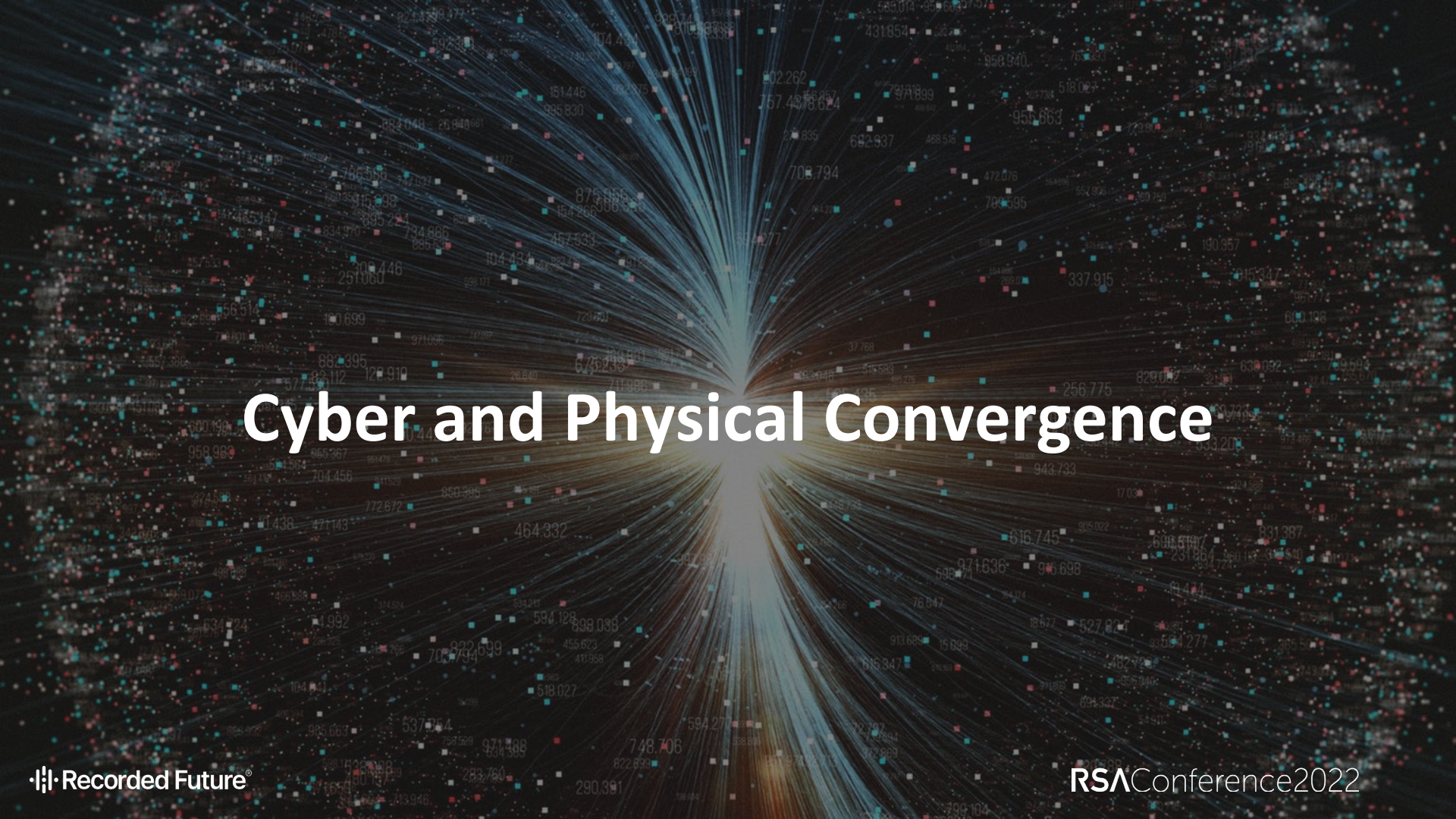
Humanity Has Become a Sensor

Recorded Future®


Recorded Future®


EPIC
MIGRATION IN
PLAY


ORACLE
SAP
aws
Tencent Cloud
salesforce
Recorded Future


Cyber and Physical Convergence

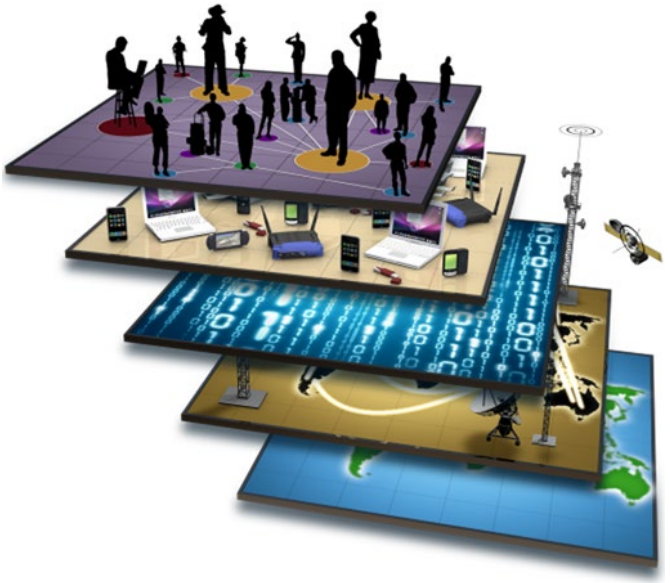

In a world of aggressive uncertainty,
intelligence is the only equalizer.

Our Original Idea

- Build a threat-oriented “digital twin” of the world
- Organize for analytics – human and algorithmic
- Enable threat analyst centaurs

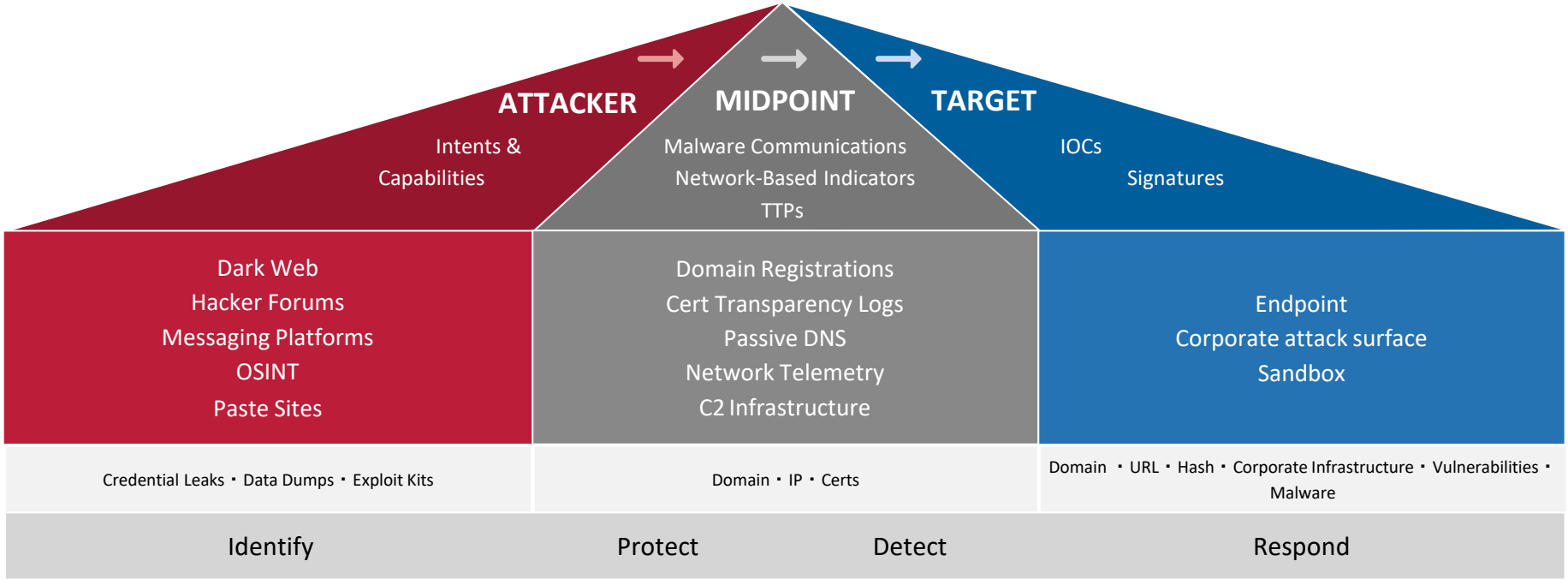
Intelligence Is Not Just For The Government

The Operating Space is Vast, and We All Operate It



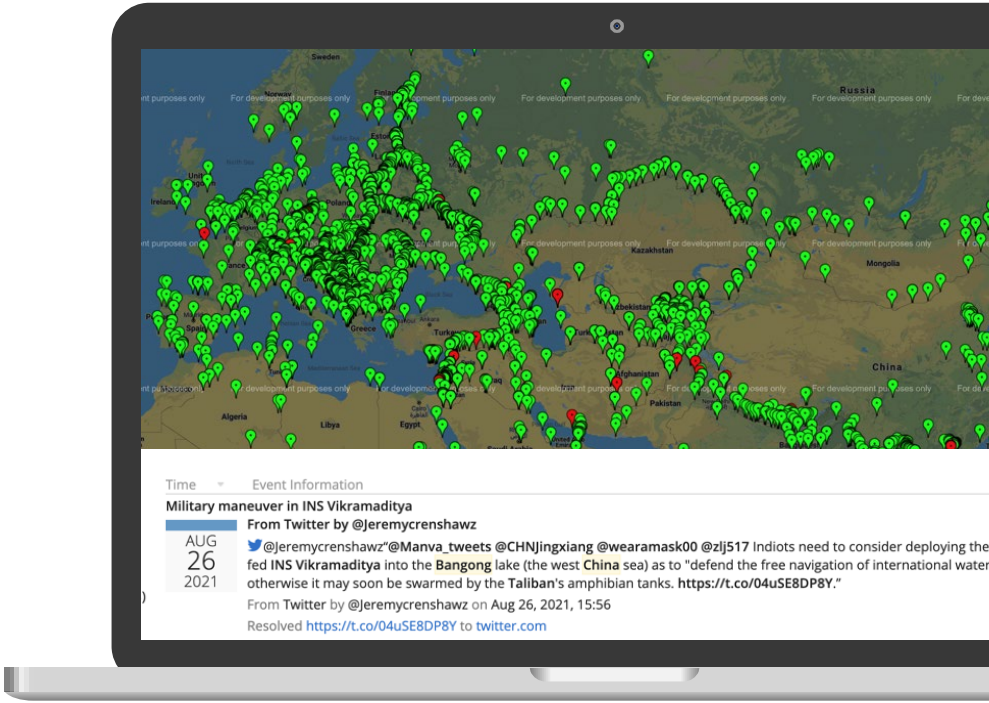
End-to-End View of Threats

Visibility From Attackers Through Midpoint to Targets



Imagery Intelligence for Deeper Context and Visual Confirmation

Now available in the Threat Intelligence and Geopolitical Intelligence modules and to Advanced license holders



Adversaries Building For Scale

Blurring lines, optimizing for unpredictability

IMAGE: EUROPOL

Catalin Cimpanu | November 8, 2021

Europol: Seven REvil/GandCrab ransomware affiliates were arrested in 2021

Ransomware gangs outsource operations

- Affiliate programs
- Commercial contractors
- Malware vendors
- Freelancers

Change in actor behaviour

→ Change in defensive strategies

Situational Awareness Requires Internal and External Perception

RSAConference2022

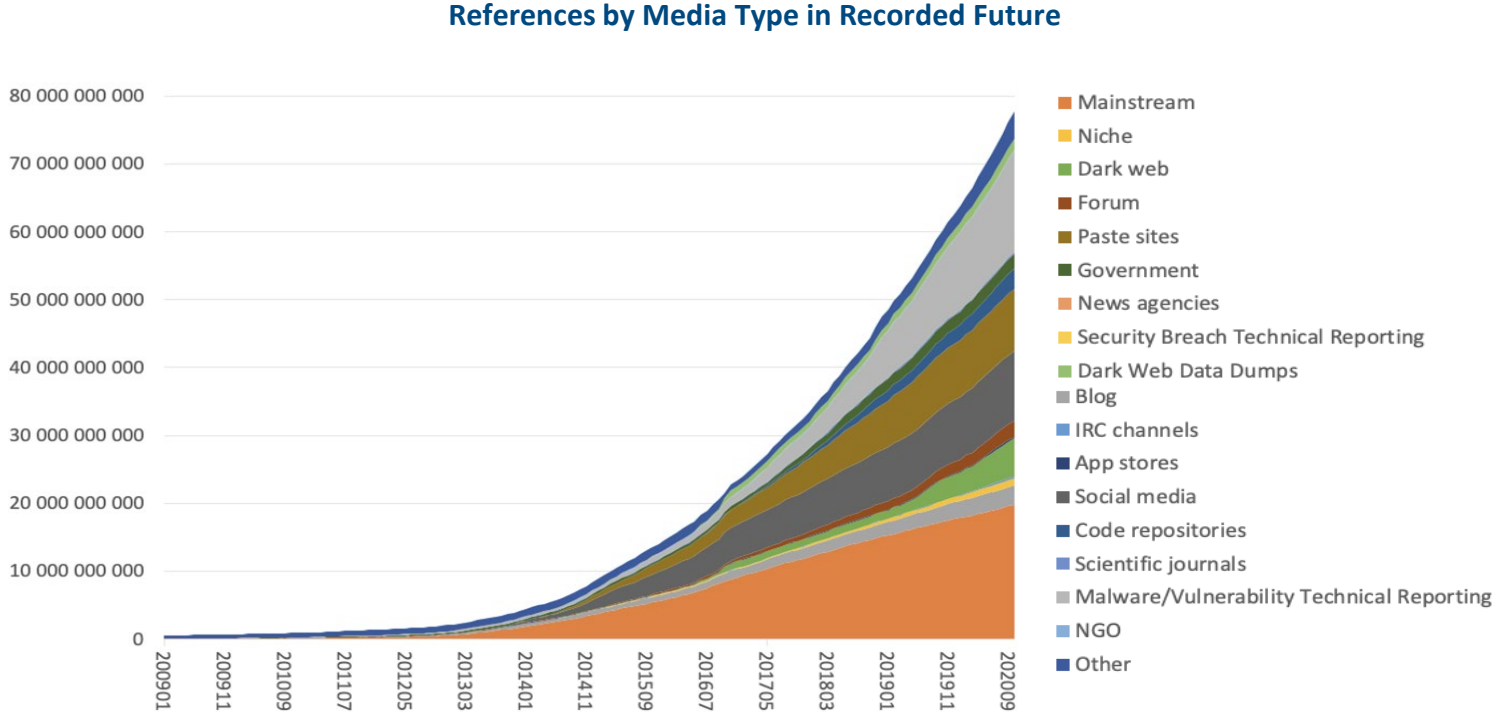
Ultimately, What is Our Mission?

Recorded Future®

What Does Everyone Need?

- WHO
- WHAT
- WHERE
- WHEN
- HOW

Growth of Recorded Future's Collection



Disparate Sources of Threat Data

Current Emotet Epoch 1 C2 as of 2020-01-17: **119.59.124.163**:8080

Source: PasteBin

Электронные письма содержали вредоносный документ **Microsoft Word**, который при открытии пытался загрузить **Emotet** на компьютер жертвы

Source: cyber-safety.ru

United Nations targeted with **Emotet Malware Phishing attack**

Source: Twitter

A new **Emotet** campaign has been observed by the Cofense Labs sending malicious emails with a Christmas themed subject to entice victims to open the attachment

Source: BleepingComputer

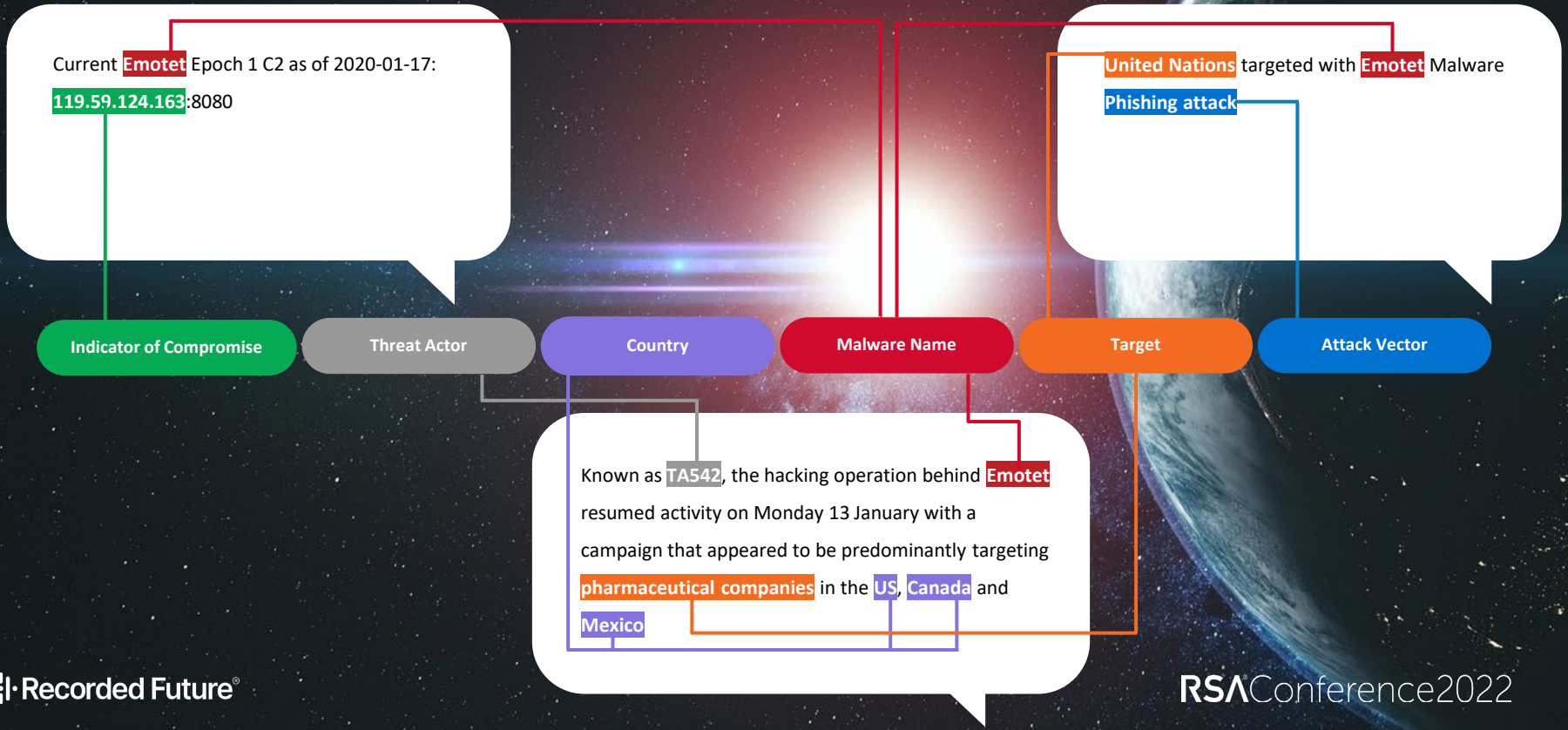
Known as **TA542**, the hacking operation behind **Emotet** resumed activity on Monday 13 January with a campaign that appeared to be predominantly targeting pharmaceutical companies in the **US**, **Canada** and **Mexico**

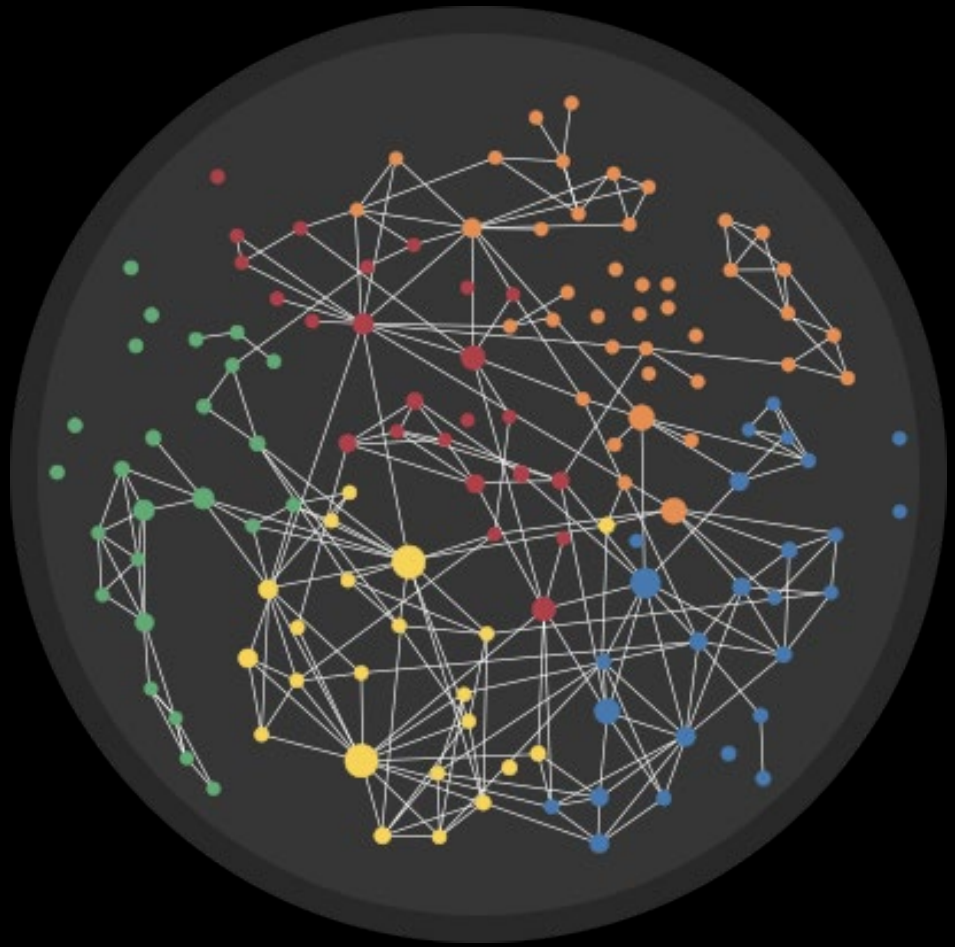
Source: ZDNet

Aktuell werden gefälschte "sichere E-Mails" mit angeblichen Rechnungen zur Verbreitung der #Schadsoftware **#Emotet** versendet. Nicht den Link in der E-Mail öffnen!

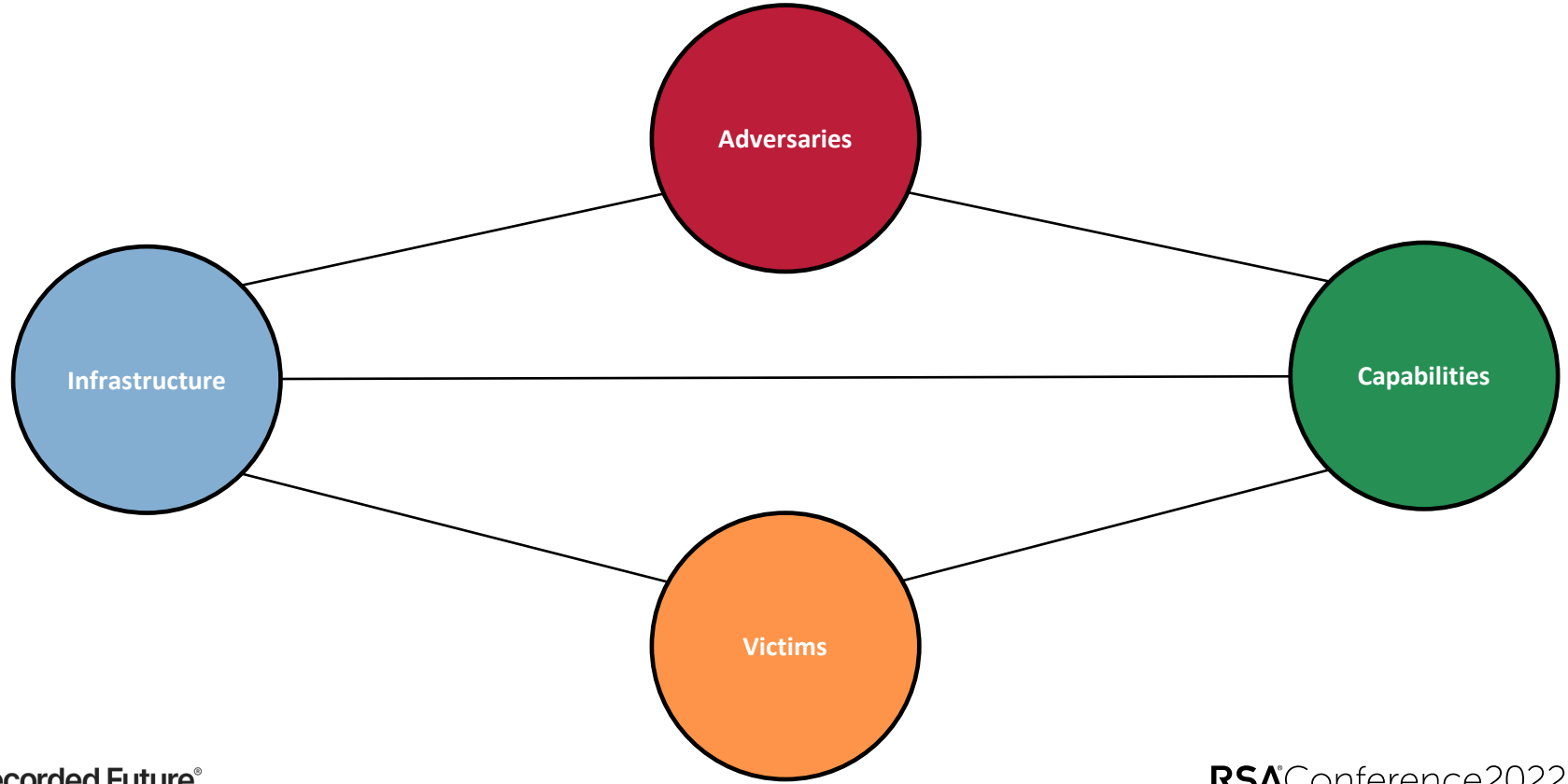
Source: CERT-BUND Twitter

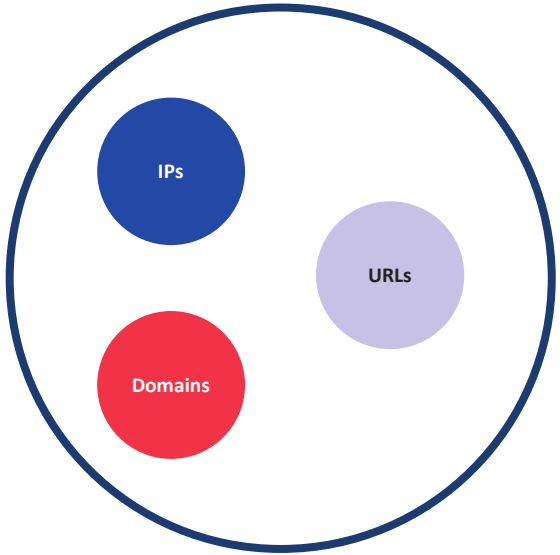
Automated Activities to Generate Intelligence





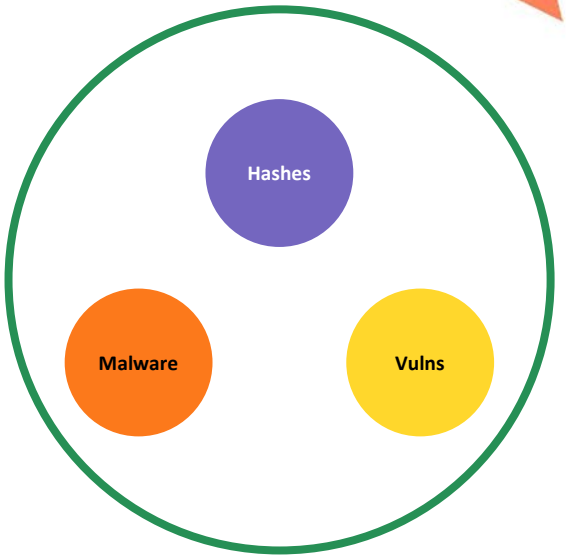
Entity Categories in the Security Intelligence Graph





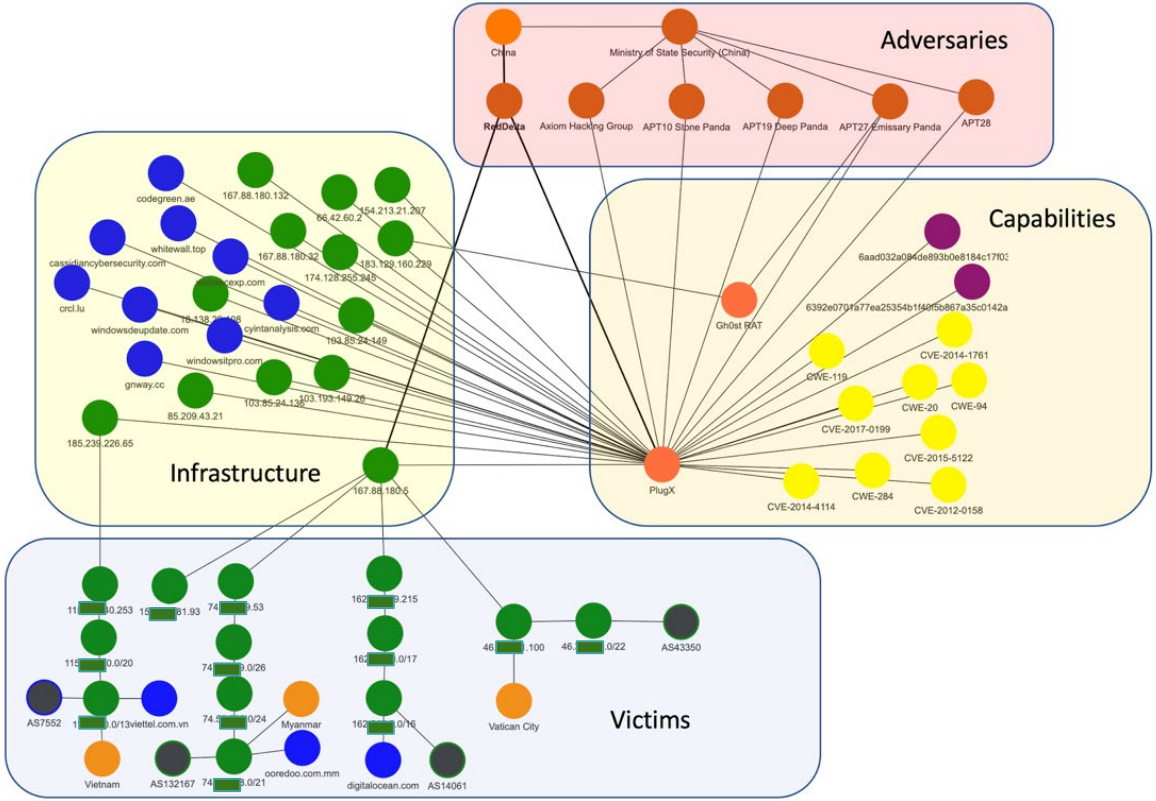
Infrastructure

Adversaries



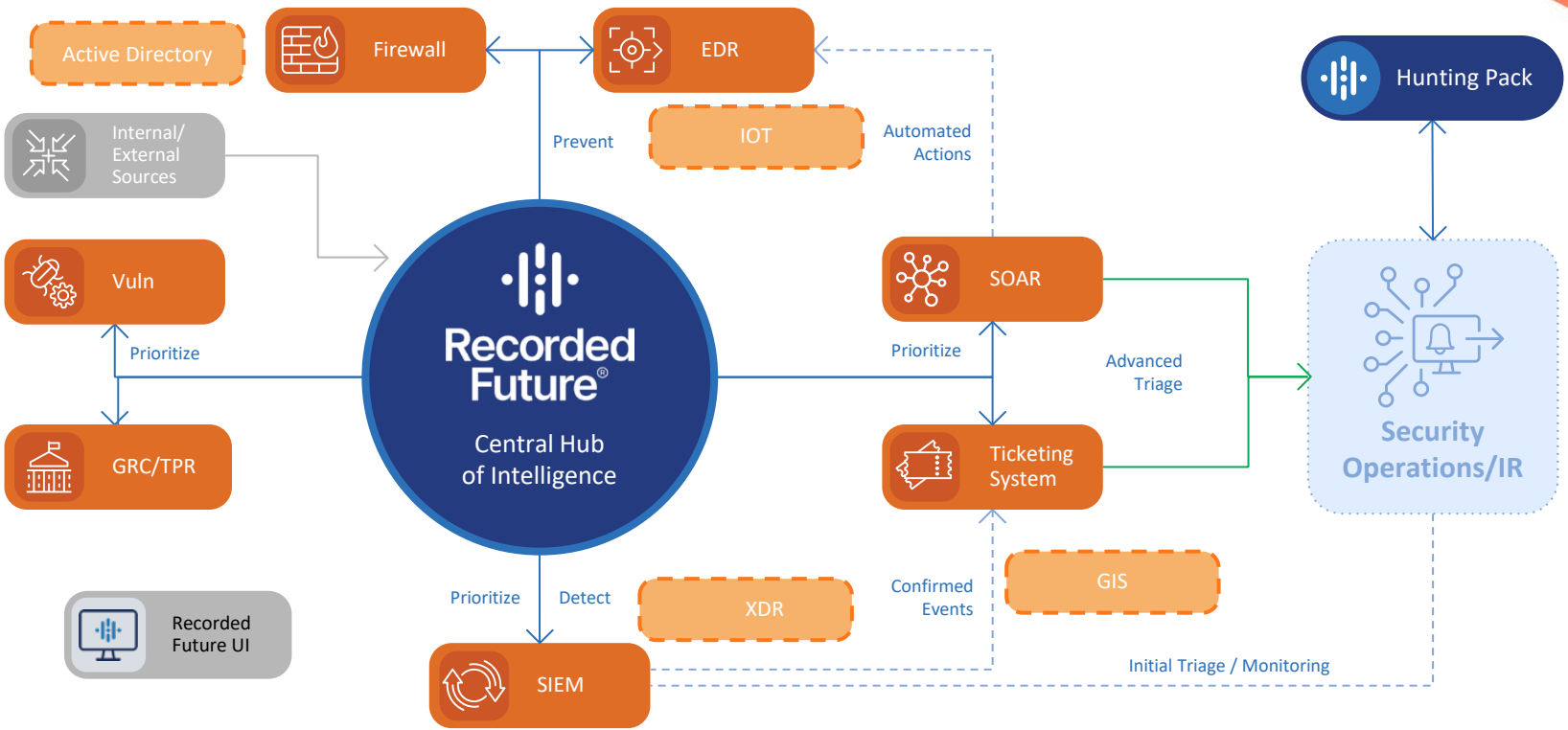
Capabilities

Victims


Adversaries
China
Ministry of State Security (China)
RedDelta
Axiom Hacking Group
APT10 Stone Panda
APT19 Deep Panda
APT27 Emissary Panda
APT28
Capabilities
Gh0st RAT
6aad032a084de893b0e8184c17f03
6392e0701a77ea25354b1f40f5b867a35c0142a
CVE-2014-1761
CWE-119
CWE-20
CWE-94
CVE-2017-0199
CVE-2015-5122
CWE-284
CVE-2014-4114
CVE-2012-0158
PlugX
Infrastructure
codegreen.ae
167.88.180.132
66.42.60.2
154.213.21.207
whitewall.top
cassidiancybersecurity.com
167.88.180.32
183.129.160.229
174.128.255.249
crcl.lu
windowsdeupdate.com
cyintanalysis.com
103.85.24.149
windowsitpro.com
gnway.cc
103.85.24.136
103.193.149.26
85.209.43.21
185.239.226.65
167.88.180.5
Victims
AS43350
AS7552
viettel.com.vn
Myanmar
Vatican City
Vietnam
AS132167
ooredoo.com.mm
digitalocean.com
AS14061

SECURITY INTELLIGENCE: QUICKLY IDENTIFY, PRIORITIZE, AND ACTION THREATS WITH CONFIDENCE

Maximize the value of existing security investments


Active Directory
Firewall
EDR
Hunting Pack
Internal/ External Sources
Prevent
IOT
Automated Actions
Vuln
Recorded Future®
Central Hub of Intelligence
SOAR
Prioritize
Prioritize
Advanced Triage
Security Operations/IR
GRC/TPR
Ticketing System
Recorded Future UI
Prioritize
Detect
XDR
Confirmed Events
GIS
SIEM
Initial Triage / Monitoring


Why it’s worthwhile to manage risk beyond audit compliance and do so while working as a team


How intelligence informs strategic security priorities and reduces uncertainty

“The question has shifted from ‘How much is enough?’ (Gordon and Loeb’s 2002 model) to ‘Where and when to invest?’ Uncertainty also plays a key role in the timing of security investments, having an effect on the choice of proactive and reactive protection measures.”

– Economic aspects of national cyber security strategies (Brangetto & Aubyn, 2015)

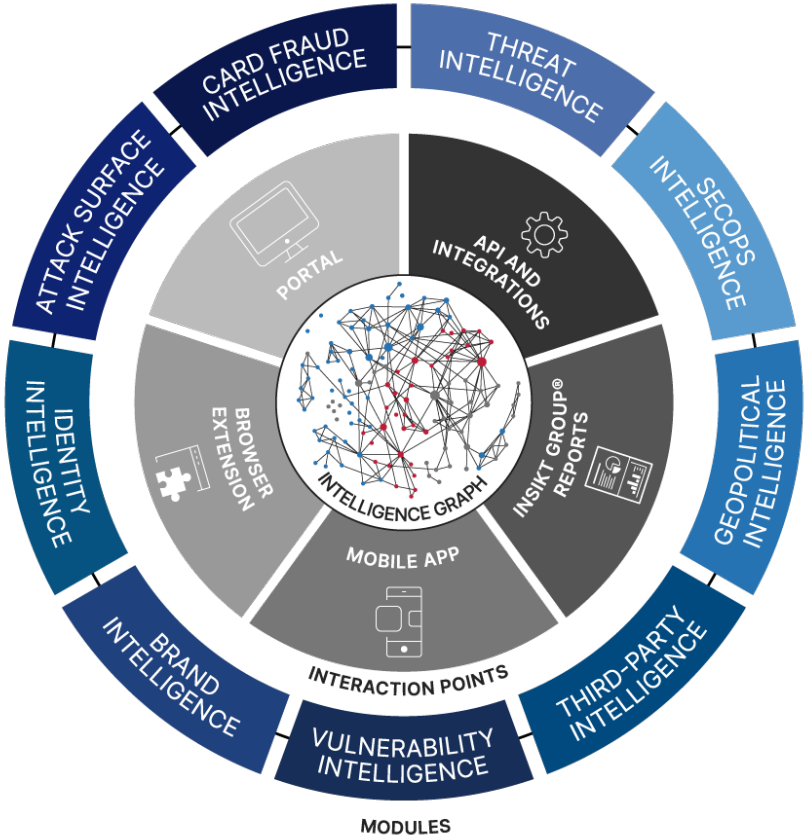
Why automation in intelligence is critical to creating measurable operational outcomes

Image Source: coscon.princeton.edu

Applying Intelligence Across the Enterprise

- Threat Intelligence Production
- Vulnerability Management
- Sec Ops
- Prioritization
- Enrichment and Correlation
- Incident Response
- Threat Hunting
- Informed Emulation and Testing
- Perspective and Focus
- Third-party Risk
- Fraud
- Identity and Access Management
- Business Operations
- Physical Safety
- Supply Chain Management
- Strategic Intelligence
- Brand Management
- Planning/Strategy/Architecture
- Fusion Center Use Cases
- Decision Advantage

The Opportunity Lies in Moving Beyond The SOC



	Brand	Attack Surface	Physical	SecOps	Vulnerability	Fraud	Identity	3rd Party	Threat
Intelligence	• Phishing domains • Malicious apps • Code leaks • DW access advertising	• Internet inventory • Asset exposures	• Terrorist campaigns • Executive/ asset threats • Travel risk	• IOA/IOC context & enrichment • Infrastructure compromises	• Active exploitation • Pre-NVD • Pre-CVSS	• Stolen payment cards • Merchant breaches • Proxy/VPN use	• Stolen credentials / tokens	• Vendor / supplier exposure analytics	• Adversary prioritization • Hunting packages • New “tools” / TTPs
Consumption	• Email reporting • API	• API system integration • Email Alerting	• Alerting • Geospatial monitoring • API system integration	• Browser extension • System of record integration	• Scanner integration • System of record integration	• API system integrations • Manual reporting	• API for SOAR playbook	• System of record integration • Intelligence cards	• Red team scenarios • Hunting team scenarios
Outcomes	• Domain / social media / app store takedowns • Legal action	• Exposed asset remediation	• Site security • Business continuity response • Executive protection	• Quicker event verdicts • Faster incident triage • Detect/block control actions	• Patch prioritization	• Active cards flagged • Account takeover prevention	• Active Directory account resets	• Vendor / supplier contract auditing / enforcement	• Security control validation • Internal threat discovery • Trend identification
KPIs	• Mean Time to Remove • ROSI	• New assets discovered • ROSI	• Physical / operational system disruption • ROSI	• Correlated detection events • ROSI	• Patch escalation • ROSI	• Cost of fraud • Approved vs declined transactions • ROSI	• Mean Time to Identify • ROSI	• Exposure identification • ROSI	• Mean Time to Assess • Mean Time to Deploy • ROSI
Risk Briefing	• NIST CSF: DE.CM-5 DE.CM-7 • Reputation management	• NIST CSF: ID.AM1-4 • Reduce breach probability • Risk reduction	• NIST CSF: DE.CM2-3 • Improve resilience	• NIST CSF: DE.AE2-3 DE.CM-1 • Improve resilience • Regulatory compliance	• NIST CSF: ID.RA-1 PR.IP-12 • PCI DSS • Regulatory compliance	• PCI DSS • Regulatory Compliance • Improve brand equity	• NIST CSF: PR.AC1-7 • Risk reduction • Regulatory compliance	• NIST CSF: ID.SC1-5 DE.CM-6 • Risk reduction • Regulatory compliance	• NIST CSF: ID.RA2-5 DE.CM-4 • Improve risk assessments

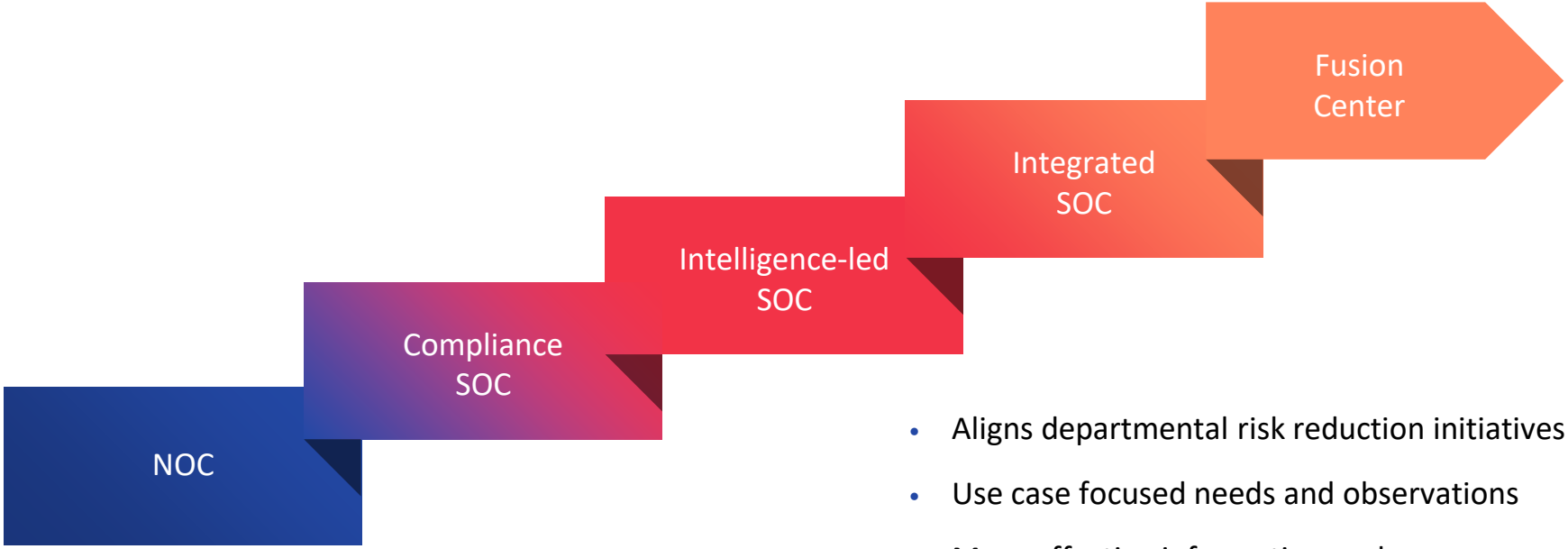
	Brand	Attack Surface	Physical	SecOps	Vulnerability	Fraud	Identity	3rd Party	Threat
Intelligence	• Phishing domains • Malicious apps • Code leaks • DW access advertising	• Internet inventory • Asset exposures	• Terrorist campaigns • Executive/ asset threats • Travel risk	• IOA/IOC context & enrichment • Infrastructure compromises	• Active exploitation • Pre-NVD • Pre-CVSS	• Stolen payment cards • Merchant breaches • Proxy/VPN use	• Stolen credentials / tokens	• Vendor / supplier exposure analytics	• Adversary prioritization • Hunting packages • New “tools” / TTPs
Consumption	• Email reporting • API	• API system integration • Email Alerting	• Alerting • Geospatial monitoring • API system integration	• Browser extension • System of record integration	• Scanner integration • System of record integration	• API system integrations • Manual reporting	• API for SOAR playbook	• System of record integration • Intelligence cards	• Red team scenarios • Hunting team scenarios
Outcomes	• Domain / social media / app store takedowns • Legal action	• Exposed asset remediation	• Site security • Business continuity response • Executive protection	• Quicker event verdicts • Faster incident triage • Detect/block control actions	• Patch prioritization	• Active cards flagged • Account takeover prevention	• Active Directory account resets	• Vendor / supplier contract auditing / enforcement	• Security control validation • Internal threat discovery • Trend identification
KPIs	• Mean Time to Remove • ROSI	• New assets discovered • ROSI	• Physical / operational system disruption • ROSI	• Correlated detection events • ROSI	• Patch escalation • ROSI	• Cost of fraud • Approved vs declined transactions • ROSI	• Mean Time to Identify • ROSI	• Exposure identification • ROSI	• Mean Time to Assess • Mean Time to Deploy • ROSI
Risk Briefing	• NIST CSF: DE.CM-5 DE.CM-7 • Reputation management	• NIST CSF: ID.AM1-4 • Reduce breach probability • Risk reduction	• NIST CSF: DE.CM2-3 • Improve resilience	• NIST CSF: DE.AE2-3 DE.CM-1 • Improve resilience • Regulatory compliance	• NIST CSF: ID.RA-1 PR.IP-12 • PCI DSS • Regulatory compliance	• PCI DSS • Regulatory Compliance • Improve brand equity	• NIST CSF: PR.AC1-7 • Risk reduction • Regulatory compliance	• NIST CSF: ID.SC1-5 DE.CM-6 • Risk reduction • Regulatory compliance	• NIST CSF: ID.RA2-5 DE.CM-4 • Improve risk assessments

	Brand	Attack Surface	Physical	SecOps	Vulnerability	Fraud	Identity	3rd Party	Threat
Intelligence	• Phishing domains • Malicious apps • Code leaks • DW access advertising	• Internet inventory • Asset exposures	• Terrorist campaigns • Executive/ asset threats • Travel risk	• IOA/IOC context & enrichment • Infrastructure compromises	• Active exploitation • Pre-NVD • Pre-CVSS	• Stolen payment cards • Merchant breaches • Proxy/VPN use	• Stolen credentials / tokens	• Vendor / supplier exposure analytics	• Adversary prioritization • Hunting packages • New “tools” / TTPs
Consumption	• Email reporting • API	• API system integration • Email Alerting	• Alerting • Geospatial monitoring • API system integration	• Browser extension • System of record integration	• Scanner integration • System of record integration	• API system integrations • Manual reporting	• API for SOAR playbook	• System of record integration • Intelligence cards	• Red team scenarios • Hunting team scenarios
Outcomes	• Domain / social media / app store takedowns • Legal action	• Exposed asset remediation	• Site security • Business continuity response • Executive protection	• Quicker event verdicts • Faster incident triage • Detect/block control actions	• Patch prioritization	• Active cards flagged • Account takeover prevention	• Active Directory account resets	• Vendor / supplier contract auditing / enforcement	• Security control validation • Internal threat discovery • Trend identification
KPIs	• Mean Time to Remove • ROSI	• New assets discovered • ROSI	• Physical / operational system disruption • ROSI	• Correlated detection events • ROSI	• Patch escalation • ROSI	• Cost of fraud • Approved vs declined transactions • ROSI	• Mean Time to Identify • ROSI	• Exposure identification • ROSI	• Mean Time to Assess • Mean Time to Deploy • ROSI
Risk Briefing	• NIST CSF: DE.CM-5 DE.CM-7 • Reputation management	• NIST CSF: ID.AM1-4 • Reduce breach probability • Risk reduction	• NIST CSF: DE.CM2-3 • Improve resilience	• NIST CSF: DE.AE2-3 DE.CM-1 • Improve resilience • Regulatory compliance	• NIST CSF: ID.RA-1 PR.IP-12 • PCI DSS • Regulatory compliance	• PCI DSS • Regulatory Compliance • Improve brand equity	• NIST CSF: PR.AC1-7 • Risk reduction • Regulatory compliance	• NIST CSF: ID.SC1-5 DE.CM-6 • Risk reduction • Regulatory compliance	• NIST CSF: ID.RA2-5 DE.CM-4 • Improve risk assessments

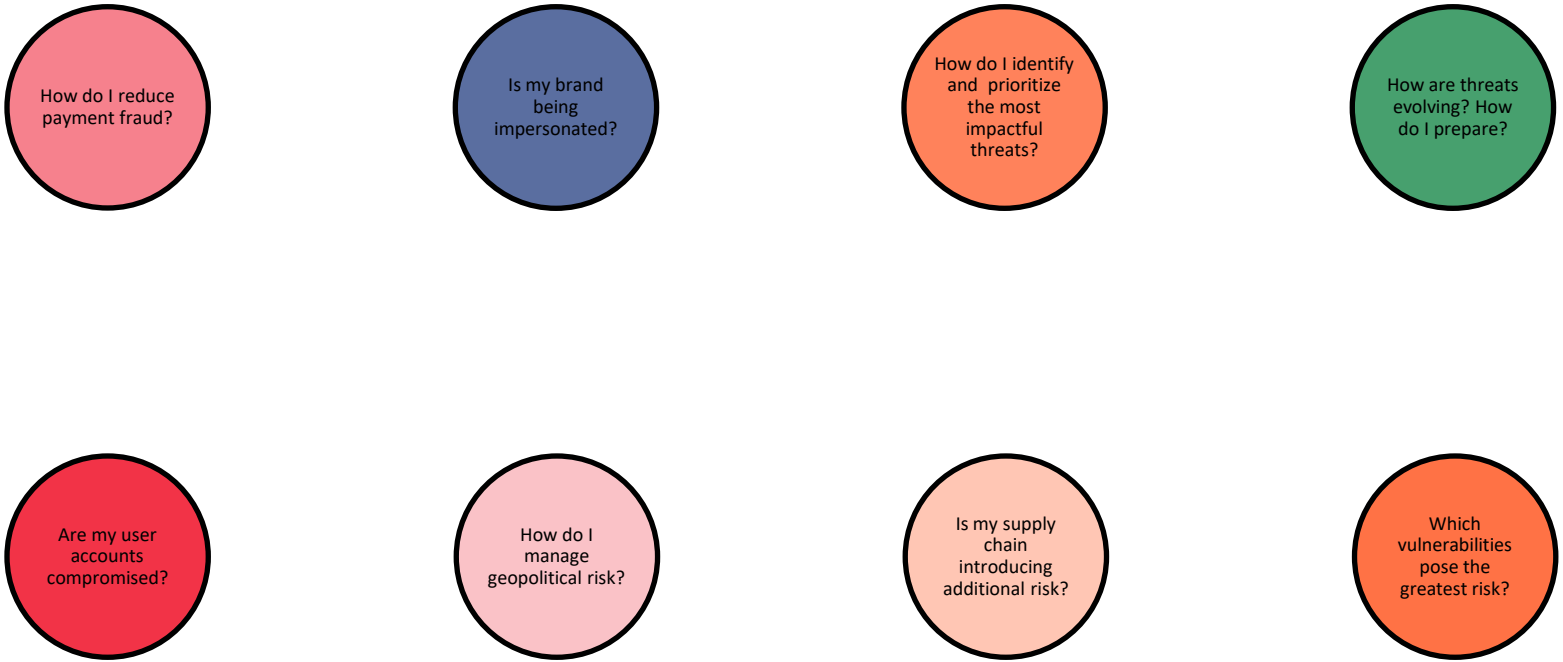
	Brand	Attack Surface	Physical	SecOps	Vulnerability	Fraud	Identity	3rd Party	Threat
Intelligence	• Phishing domains • Malicious apps • Code leaks • DW access advertising	• Internet inventory • Asset exposures	• Terrorist campaigns • Executive/ asset threats • Travel risk	• IOA/IOC context & enrichment • Infrastructure compromises	• Active exploitation • Pre-NVD • Pre-CVSS	• Stolen payment cards • Merchant breaches • Proxy/VPN use	• Stolen credentials / tokens	• Vendor / supplier exposure analytics	• Adversary prioritization • Hunting packages • New “tools” / TTPs
Consumption	• Email reporting • API	• API system integration • Email Alerting	• Alerting • Geospatial monitoring • API system integration	• Browser extension • System of record integration	• Scanner integration • System of record integration	• API system integrations • Manual reporting	• API for SOAR playbook	• System of record integration • Intelligence cards	• Red team scenarios • Hunting team scenarios
Outcomes	• Domain / social media / app store takedowns • Legal action	• Exposed asset remediation	• Site security • Business continuity response • Executive protection	• Quicker event verdicts • Faster incident triage • Detect/block control actions	• Patch prioritization	• Active cards flagged • Account takeover prevention	• Active Directory account resets	• Vendor / supplier contract auditing / enforcement	• Security control validation • Internal threat discovery • Trend identification
KPIs	• Mean Time to Remove • ROSI	• New assets discovered • ROSI	• Physical / operational system disruption • ROSI	• Correlated detection events • ROSI	• Patch escalation • ROSI	• Cost of fraud • Approved vs declined transactions • ROSI	• Mean Time to Identify • ROSI	• Exposure identification • ROSI	• Mean Time to Assess • Mean Time to Deploy • ROSI
Risk Briefing	• NIST CSF: DE.CM-5 DE.CM-7 • Reputation management	• NIST CSF: ID.AM1-4 • Reduce breach probability • Risk reduction	• NIST CSF: DE.CM2-3 • Improve resilience	• NIST CSF: DE.AE2-3 DE.CM-1 • Improve resilience • Regulatory compliance	• NIST CSF: ID.RA-1 PR.IP-12 • PCI DSS • Regulatory compliance	• PCI DSS • Regulatory Compliance • Improve brand equity	• NIST CSF: PR.AC1-7 • Risk reduction • Regulatory compliance	• NIST CSF: ID.SC1-5 DE.CM-6 • Risk reduction • Regulatory compliance	• NIST CSF: ID.RA2-5 DE.CM-4 • Improve risk assessments

	Brand	Attack Surface	Physical	SecOps	Vulnerability	Fraud	Identity	3rd Party	Threat
Intelligence	• Phishing domains • Malicious apps • Code leaks • DW access advertising	• Internet inventory • Asset exposures	• Terrorist campaigns • Executive/ asset threats • Travel risk	• IOA/IOC context & enrichment • Infrastructure compromises	• Active exploitation • Pre-NVD • Pre-CVSS	• Stolen payment cards • Merchant breaches • Proxy/VPN use	• Stolen credentials / tokens	• Vendor / supplier exposure analytics	• Adversary prioritization • Hunting packages • New “tools” / TTPs
Consumption	• Email reporting • API	• API system integration • Email Alerting	• Alerting • Geospatial monitoring • API system integration	• Browser extension • System of record integration	• Scanner integration • System of record integration	• API system integrations • Manual reporting	• API for SOAR playbook	• System of record integration • Intelligence cards	• Red team scenarios • Hunting team scenarios
Outcomes	• Domain / social media / app store takedowns • Legal action	• Exposed asset remediation	• Site security • Business continuity response • Executive protection	• Quicker event verdicts • Faster incident triage • Detect/block control actions	• Patch prioritization	• Active cards flagged • Account takeover prevention	• Active Directory account resets	• Vendor / supplier contract auditing / enforcement	• Security control validation • Internal threat discovery • Trend identification
KPIs	• Mean Time to Remove • ROSI	• New assets discovered • ROSI	• Physical / operational system disruption • ROSI	• Correlated detection events • ROSI	• Patch escalation • ROSI	• Cost of fraud • Approved vs declined transactions • ROSI	• Mean Time to Identify • ROSI	• Exposure identification • ROSI	• Mean Time to Assess • Mean Time to Deploy • ROSI
Risk Briefing	• NIST CSF: DE.CM-5 DE.CM-7 • Reputation management	• NIST CSF: ID.AM1-4 • Reduce breach probability • Risk reduction	• NIST CSF: DE.CM2-3 • Improve resilience	• NIST CSF: DE.AE2-3 DE.CM-1 • Improve resilience • Regulatory compliance	• NIST CSF: ID.RA-1 PR.IP-12 • PCI DSS • Regulatory compliance	• PCI DSS • Regulatory Compliance • Improve brand equity	• NIST CSF: PR.AC1-7 • Risk reduction • Regulatory compliance	• NIST CSF: ID.SC1-5 DE.CM-6 • Risk reduction • Regulatory compliance	• NIST CSF: ID.RA2-5 DE.CM-4 • Improve risk assessments

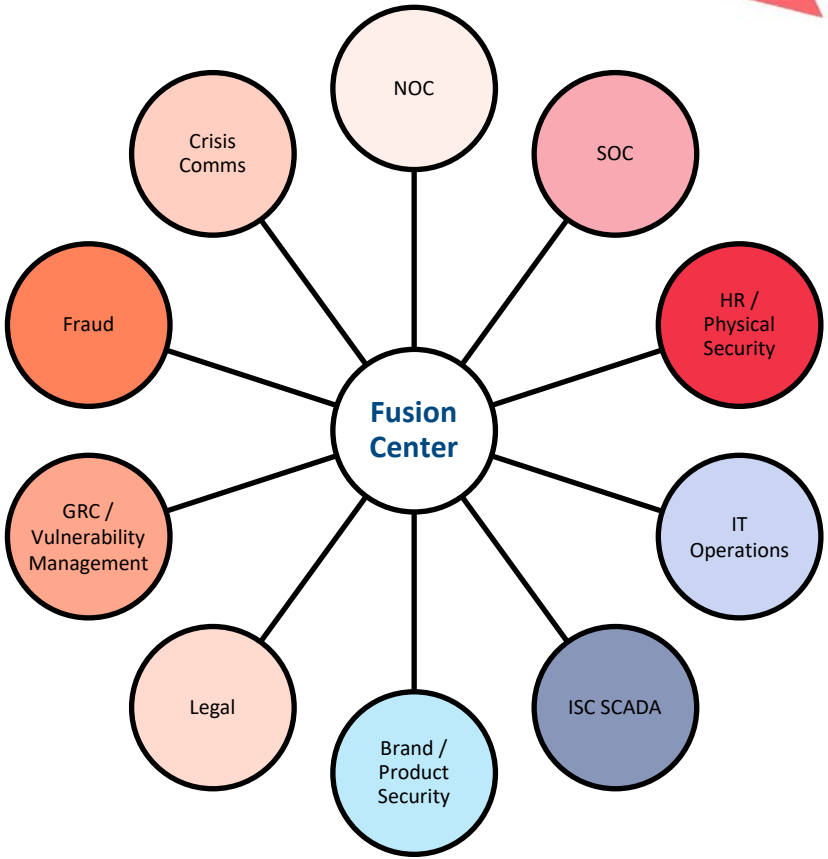
The Evolution of Intel-led Security



- Aligns departmental risk reduction initiatives
- Use case focused needs and observations
- More effective information exchange
- Streamlines response


How do I reduce payment fraud?
Is my brand being impersonated?
How do I identify and prioritize the most impactful threats?
How are threats evolving? How do I prepare?
Are my user accounts compromised?
How do I manage geopolitical risk?
Is my supply chain introducing additional risk?
Which vulnerabilities pose the greatest risk?

Intel Informs Risk Decisions **Beyond** The SOC



- Ensure delivery of **timely and objective** national intelligence
- Establish **objectives and priorities** for collection, analysis, production and dissemination of national intelligence
- Ensure **maximum availability** of and access to intelligence information within the Intelligence Community

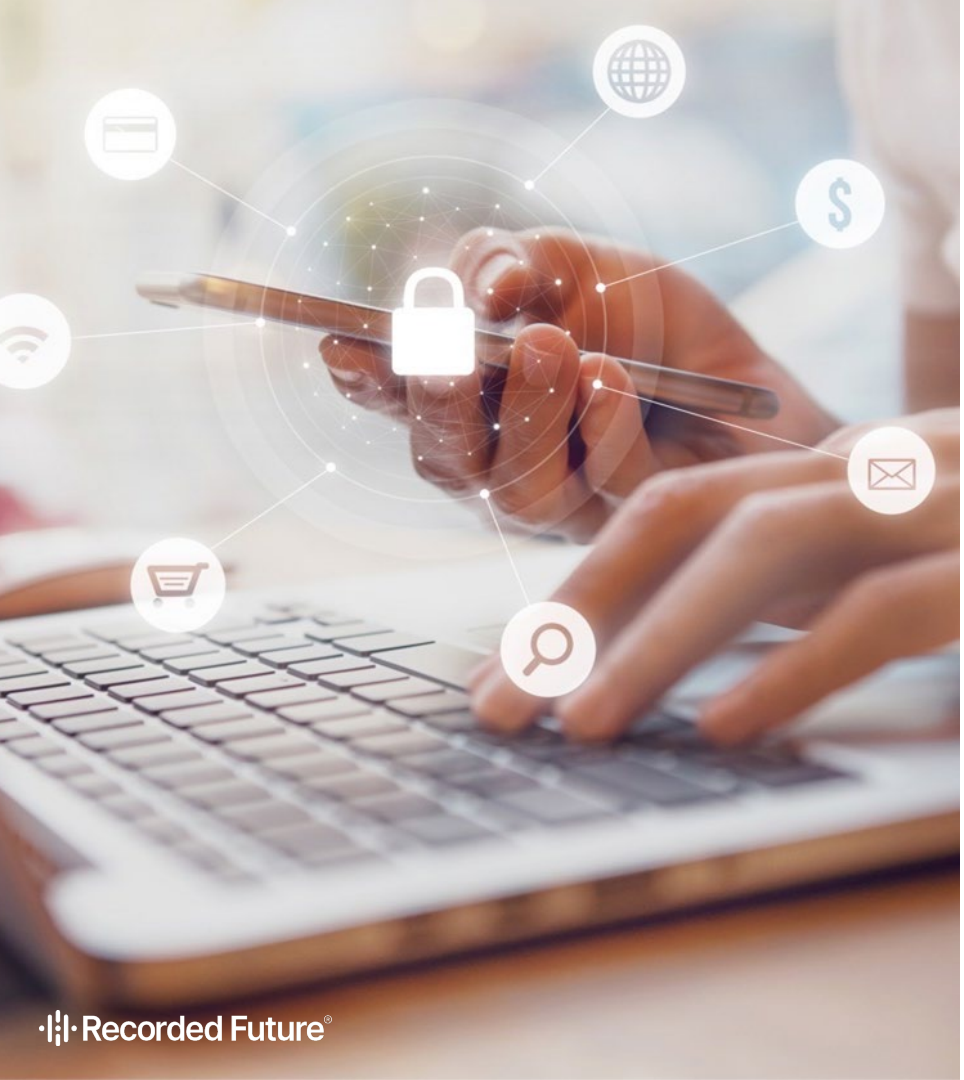
Intelligence Fusion Happens Every Day in Our Security Activities

Recorded Future®

- Impacts end-users before SOC is aware
- Users contact help desk
- Help desk lacks escalation path
- No incident response playbook
- Unclear operational impacts
- Crisis communications
- Brand impacts

- Innumerable vulnerabilities exist
- Identifying exploitable technology is difficult
- Unclear how to prioritize patching
- Business justification difficulties
- Operational impacts

- Who do you trust?
- Is this request legitimate?
- Re-used Credentials
- Few boundaries between work and personal computing environments
- Exposed Credentials are prevalent
- No honor among thieves



- What is my exposure?
- Difficulty identifying problems early
- Should I trust this credential?
- Huge volumes to deal with
- Business process disruption and cost
- Client dissatisfaction

- Access to privileged information
- Frequently connect from unsecured locations
- Strapped for time
- Impersonation to gain access to confidential information
- Bad-guys take advantage of social media

- Third parties provide a gateway into the network
- What is my exposure?
- Difficulty identifying problems early
- Difficult to assess their security posture
- Not always disclosed when they are breached

- Temporal and location bound threats
- Nexus between the physical and logical threat environments
- Are my facilities or people in danger?
- Supply chain disruptions
- Business continuity

RSAConference2022

Decision Advantage!

Recorded Future®

The Bottom Line Up Front

- Why it's worthwhile to manage risk beyond audit compliance
  (hint: the accelerating convergence of the physical and cyber worlds)
- How intelligence informs strategic security priorities and reduces uncertainty
- Building scalable and consumable intelligence
- Why automation in intelligence is critical to creating measurable operational outcomes
- We need to expand the paradigm for the use cases of intelligence

Image Source: coscon.princeton.edu

RSAConference2022

Thank You!

Stu Solomon

Stuart.Solomon@recordedfuture.com