- **IntelMind Cyber DD**

CYBER DUE DILIGENCE REPORT · M&A

Acme Industries Corp

Full outside-in cyber-risk analysis of the target company. 10 Key Risk Indicators (KRIs), 130+ sources queried. Verifiable by RFC 3161 timestamp.

JURISDICTION

Estados Unidos

DOMAIN

Acme Industries.com

IDENTIFIERS

CIK 9999999999 · LEI 0000ACME00CDFSAMPLE00 · EIN 00-0000000 · Reg. ACME-PUBLIC-SAMPLE

ANALYSIS DATE

September 19, 2026 at 3:49 PM

CONFIDENTIAL · RECIPIENT ONLY

IMD-CDF-MU8KBTND-YUDF

EXECUTIVE SUMMARY

One-page verdict

For executives · 30-second read · Go/No-Go decision

16

GLOBAL CYBER RISK: LOW

Low overall risk — 2 medium-priority exposures to remediate pre-close.

Weighted average of 10 KRIs (Key Risk Indicators) covering cybersecurity, executive exposure, legal sanctions, dark-web leaks and typosquatting. 10/10 indicators successfully evaluated.

0	2	8	0
CRITICAL	MEDIUM	LOW	CLEAN

MAP OF THE 10 INDICATORS

01 **Executive Digital Exposure** — 44

El equipo directivo de Acme Industries Corp está públicamente identificado — lis...

02 **Known Breaches & Credentials** — 23

Exposición de credenciales de usuarios/terceros externos de Acme Industries

03 **DNS Weaknesses & Hygiene** — 12

Higiene de autenticación de correo mejorable en Acme Industries

04 **Perimeter Security / EASM** — 4

Sin servicios críticos expuestos en Acme Industries

05 **Reputational & Sentiment** — 0

Acme Industries Corp tiene cobertura de prensa (21 artículos en 12 meses) sin se...

06 **Legal & Regulatory** — 0

Acme Industries Corp no figura en las listas de sanciones de la OFAC (OFAC SDN L...

07 **Supply Chain Risk** — 16

Acme Industries Corp depende de 1 proveedores tecnológicos de terceros — superfi...

08 **Malicious Infrastructure / Typosquatting** — 35

9 dominios parecidos a Acme Industries

09 **Shadow IT / Code Leaks** — 0

No se detectaron ficheros que expongan Acme Industries

10 **Dark Web Intelligence** — 18

Datos asociados a Acme Industries Corp circulan en canales de cibercrimen

INDICATORS AT A GLANCE

The 10 KRIs in card format

One card per indicator showing **what we found** and **the concrete action the team should take**. Designed for rapid review and delegation to the relevant teams. Full detail and sources are in the following sections.

1 Executive Digital Exposure

PRE-CLOSE · 44/100 · MEDIUM

WHAT IT MEANS

The leadership team of Acme Industries Corp is publicly identifiable, increasing the risk of impersonation fraud targeting executives.

FINANCIAL IMPACT

€130k-2M. An attacker could impersonate an executive to defraud the company or its clients.

HOW TO FIX IT

Concienciación anti-BEC para el C-suite y barrido de su PII personal en data brokers con solicitudes de retirada.

2 Known Breaches & Credentials

PRE-CLOSE · 23/100 · LOW

WHAT IT MEANS

There are leaked login details for users associated with Acme Industries, which could allow unauthorized access to sensitive systems.

FINANCIAL IMPACT

€130k-2M. An attacker could impersonate executives and defraud the company or its clients.

HOW TO FIX IT

Forzar reseteo de las cuentas de usuario afectadas y revisar los accesos de terceros.

3 DNS Weaknesses & Hygiene

PRE-CLOSE · 12/100 · LOW

WHAT IT MEANS

Acme Industries Corp has weaknesses in its email authentication practices, making it vulnerable to impersonation attacks. This could allow malicious actors to pose as the company and defraud its customers.

FINANCIAL IMPACT

€130k-2M. An attacker could impersonate the company and trick clients into paying fraudulent invoices.

HOW TO FIX IT

Completar la autenticación de correo (DKIM / MTA-STS) y endurecer la política.

4 Perimeter Security / EASM

PRE-CLOSE 4/100 LOW

WHAT IT MEANS

The company has a large number of potential entry points due to numerous subdomains, which could be exploited by attackers before the acquisition.

FINANCIAL IMPACT

€130k-2M. An attacker could impersonate the CFO and defraud clients through fraudulent invoices.

HOW TO FIX IT

Reducir el inventario de subdominios al mínimo necesario y retirar de internet los entornos de test.

5 Reputational & Sentiment

0/100 LOW

WHAT IT MEANS

Acme Industries Corp tiene cobertura de prensa (21 artículos en 12 meses) sin señales de crisis reputacional.

HOW TO FIX IT

Sin acción reputacional inmediata. Mantener monitorización de prensa hasta el cierre.

6 Legal & Regulatory

0/100 LOW

WHAT IT MEANS

Acme Industries Corp no figura en las listas de sanciones de la OFAC (OFAC SDN List + OFAC Consolidated List) consultadas a fecha del análisis.

HOW TO FIX IT

Sin acción requerida en el cribado de sanciones OFAC.

7 Supply Chain Risk

PRE-CLOSE 16/100 LOW

WHAT IT MEANS

Acme Industries Corp relies on third-party technology providers, which introduces risks if those vendors have security issues.

FINANCIAL IMPACT

€380k-20M. A breach in the supply chain could lead to significant fines and reputational damage.

HOW TO FIX IT

Inventariar los proveedores críticos, revisar sus certificaciones de seguridad y exigir cláusulas de ciberseguridad en sus contratos antes del cierre.

8 Malicious Infrastructure / Typosquatting

PRE-CLOSE 35/100 MEDIUM

WHAT IT MEANS

There are several lookalike domains that could be used to impersonate Acme Industries, posing a risk of fraud and brand damage.

FINANCIAL IMPACT

€130k-2M. An attacker could impersonate the company to defraud clients or siphon funds.

HOW TO FIX IT

Verificar por WHOIS la titularidad, monitorizar los dominios y registrar defensivamente las variantes críticas que sigan libres.

9 Shadow IT / Code Leaks

0/100 LOW

WHAT IT MEANS

No se detectaron ficheros que expongan Acme Industries.com en contextos de secreto (.env, credenciales) en GitHub.

HOW TO FIX IT

Sin acción inmediata. Mantener vigilancia de repositorios públicos.

10 Dark Web Intelligence

PRE-CLOSE 18/100 LOW

WHAT IT MEANS

Data related to Acme Industries is being sold on criminal networks, indicating a potential risk of cyberattacks shortly after acquisition.

FINANCIAL IMPACT

€1-3M. An attacker could lock up the company's systems and demand a ransom.

HOW TO FIX IT

Vigilar los canales de cibercrimen y, para una due diligence M&A completa, activar un feed de inteligencia de dark web de pago.

DETAILED ANALYSIS

Analysis by indicator

For each KRI: the specific threat, deal impact, the action to take (or several where applicable), numbered individual findings and a recommendation tailored to this company.

KRI 1 Executive Digital Exposure

44/100 MEDIUM

FOR THE INVESTOR — PRE-CLOSE

Acme Industries Corp's leadership team is publicly listed, making them vulnerable to targeted impersonation attacks. An attacker could exploit this information to pose as an executive, potentially leading to fraudulent invoice payments or unauthorized transactions. This risk is particularly significant during the M&A process, where swift financial decisions are common. Historical cases, such as the incidents faced by companies like Marriott and Target, illustrate the severe financial impact of such fraud. Addressing this exposure is critical to safeguarding the company's assets and reputation.

FINANCIAL IMPACT **€130k-2M. An attacker could impersonate an executive to defraud the company or its clients.**

HOW TO FIX IT

Implement anti-impersonation training and personal data removal from brokers.

WHO	Mid-size cyber consultancy such as Optiv or NCC Group.
HOW	1) Conduct an initial audit of executive email exposure.,2) Provide anti-fraud training for the executive team.,3) Identify and request the removal of personal data from data brokers.,4) Establish monitoring for any future exposure.
WHEN	Before deal close.
TIME	1 month
FIX COST	**€30-80k**
DIFFICULTY	MEDIUM
SEVERITY	MEDIUM

TECHNICAL DETAIL — THREAT DETECTED

El equipo directivo de Acme Industries Corp está públicamente identificado — lista de objetivos lista para spear-phishing y suplantación de ejecutivos.

WHAT CAN HAPPEN (TECHNICAL)

Con los nombres y cargos del C-suite (públicos por mandato SEC), un atacante ensambla un paquete de targeting de precisión: spear-phishing, suplantación de ejecutivos y fraude del CEO se vuelven directamente ejecutables. La exposición se agrava si los datos personales (domicilios, móviles, familiares) figuran además en bases de data brokers — periodos de transición como una operación M&A son un disparador documentado de Business Email Compromise.

RECOMMENDED ACTION (TECHNICAL)

Concienciación anti-BEC para el C-suite y barrido de su PII personal en data brokers con solicitudes de retirada.

INDIVIDUAL FINDINGS (1)

1 **Gobierno corporativo de Acme Industries Corp públicamente identificado: 18 personas (7 con cargo ejecutivo, 10 consejeros).** Confidence 82

A partir de las declaraciones SEC (Forms 3/4) se identifican 18 miembros del gobierno corporativo con nombre y cargo. Esta información es pública por mandato regulatorio — un atacante dispone de la lista de objetivos de spear-phishing y fraude del CEO sin esfuerzo. Identificados: Julie Mchugh; Sam R Leno; Gary J Pruden; Phuong Khanh Morrow; Minnie Baylor-henry; Gerard Ber; James H Thrall; Heinz Christoph Maeusli; Ludger Dinkelborg (See Remarks); Robert J. Jr. Marshall (CFO and Treasurer); Daniel Niedzwiecki (See Remarks); Kimberly Brown (Chief Accounting Officer); Amanda Michelle Morgan (Chief Commercial Officer); Julia Marie Eastland.

TAILORED RECOMMENDATION

Plan de exposición ejecutiva para Acme Industries Corp:
1. Gobierno corporativo identificado de Acme Industries Corp (18): Julie Mchugh — Consejero; Sam R Leno — Consejero; Gary J Pruden — Consejero; Phuong Khanh Morrow — Consejero; Minnie Baylor-henry — Consejero; Gerard Ber — Consejero; James H Thrall — Consejero; Heinz Christoph Maeusli — Consejero; Ludger Dinkelborg — See Remarks; Robert J. Jr. Marshall — CFO and Treasurer; Daniel Niedzwiecki — See Remarks; Kimberly Brown — Chief Accounting Officer; Amanda Michelle Morgan — Chief Commercial Officer; Julia Marie Eastland — Consejero; Mary Anne Heino — Executive Chair; Rajiv A Patel; Paul Blanchfield — President; Partners L L C/ca Farallon.
2. Prioridad de protección — cargos de máxima exposición a fraude del CEO/BEC: Robert J. Jr. Marshall, Kimberly Brown, Amanda Michelle Morgan, Mary Anne Heino, Paul Blanchfield. Barrido de su PII personal (domicilio, móvil, familiares) en data brokers y solicitudes de retirada (opt-out).
3. Activar formación anti-BEC específica para el C-suite y verificación fuera de banda obligatoria para órdenes de pago/transferencia, especialmente durante el periodo de la operación.
4. Para cuantificar la exposición de PII personal del C-suite en data brokers se requiere activar un feed de data brokers — recomendado para completar este indicador.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
Gobierno corporativo de Acme Industries Corp públicamente identificado: 18 personas (7 con cargo ejecutivo, 10 consejeros).	SEC EDGAR (Forms 3/4)	www.sec.gov/

Overall confidence: **MEDIA** Sources queried: **1**

KRI 2

Known Breaches & Credentials

23/100 LOW

FOR THE INVESTOR — PRE-CLOSE

Acme Industries has confirmed instances of leaked login details for three users and two external partners. This exposure poses a risk of unauthorized access, potentially allowing attackers to take control of accounts and manipulate operations. If exploited, the company could face significant financial losses from fraud or operational disruptions. In the M&A context, such vulnerabilities can lead to a reduction in company valuation, as seen in past cases like Yahoo's price cut after a data breach. Addressing this issue is critical to safeguarding the company's assets and reputation.

FINANCIAL IMPACT **€130k-2M. An attacker could impersonate executives and defraud the company or its clients.**

HOW TO FIX IT

Reset the affected user accounts and review third-party access immediately.

WHO	Local managed cybersecurity team such as Arctic Wolf or Rapid7 MDR.
HOW	1) Conduct an initial audit of affected accounts.,2) Reset passwords for the compromised users.,3) Review and revoke unnecessary access for third parties.,4) Implement mandatory two-step login for all users.
WHEN	Before deal close
TIME	1 week
FIX COST	**€5-15k**
DIFFICULTY	LOW
SEVERITY	MEDIUM

TECHNICAL DETAIL — THREAT DETECTED

Exposición de credenciales de usuarios/terceros externos de Acme Industries.com en stealer logs; sin equipos de empleados comprometidos.

WHAT CAN HAPPEN (TECHNICAL)

Los empleados de la empresa no figuran comprometidos — el riesgo interno es bajo. Sí hay credenciales de usuarios externos / terceros: riesgo para las cuentas de cliente y para accesos de proveedores a las aplicaciones de la empresa.

RECOMMENDED ACTION (TECHNICAL)

Forzar reseteo de las cuentas de usuario afectadas y revisar los accesos de terceros.

INDIVIDUAL FINDINGS (2)

1 **3 usuario(s) de aplicaciones de Acme Industries.com aparecen en stealer logs.** Confidence 80

HudsonRock detecta 3 máquina(s) de usuarios externos infectadas con credenciales de acceso a aplicaciones de Acme Industries.com. Aplicaciones afectadas: https://ecommerce.Acme Industries.com/cgi-bin/lansaweb, http://visitor.Acme Industries.com/ar/Login.aspx, https://help.Acme Industries.com.

2 **2 tercero(s) con acceso relacionado con Acme Industries.com aparecen en stealer logs.** Confidence 75

HudsonRock detecta 2 máquina(s) de terceros (proveedores/colaboradores) infectadas con credenciales relacionadas con Acme Industries.com.

TAILORED RECOMMENDATION

Plan de remediación de credenciales para Acme Industries Corp (Acme Industries.com):
1. 3 usuario(s) de aplicaciones de Acme Industries.com comprometidos (https://ecommerce.Acme Industries.com/cgi-bin/lansaweb, http://visitor.Acme Industries.com/ar/Login.aspx, https://help.Acme Industries.com). Forzar reseteo de esas cuentas y activar MFA obligatorio en esas aplicaciones.
2. 2 tercero(s) con accesos comprometidos — revisar y rotar las credenciales de los proveedores/colaboradores con acceso a sistemas de Acme Industries Corp.
3. Ampliar el cribado a bases de brechas históricas (HIBP) y a la monitorización continua de nuevos stealer logs.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
3 usuario(s) de aplicaciones de Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/
2 tercero(s) con acceso relacionado con Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/

Overall confidence: **MEDIA** Sources queried: **1**

KRI 3 DNS Weaknesses & Hygiene

12/100 LOW

FOR THE INVESTOR — PRE-CLOSE

Acme Industries Corp currently has ambiguous email authentication settings, which could lead to impersonation attacks. Without strict policies in place, malicious actors could send emails that appear to come from Acme, potentially defrauding customers. This situation poses a significant risk, especially in the U.S. market, where trust is paramount. In the M&A context, such vulnerabilities can lead to financial losses and reputational damage, as seen in cases like the Marriott-Starwood merger, where security weaknesses had substantial financial implications. Addressing this issue is critical to safeguarding the company's assets and reputation post-acquisition.

FINANCIAL IMPACT

€130k-2M. An attacker could impersonate the company and trick clients into paying fraudulent invoices.

HOW TO FIX IT

Implement strict email authentication measures to enhance security.

WHO	Local managed cybersecurity team such as Arctic Wolf or Rapid7 MDR.
HOW	1) Conduct an initial audit of current email settings.,2) Configure the email authentication protocols correctly.,3) Implement strict policies for sender verification.,4) Provide training on recognizing fraudulent emails.
WHEN	Before deal close
TIME	1 week
FIX COST	**€5-15k**
DIFFICULTY	LOW
SEVERITY	MEDIUM

TECHNICAL DETAIL — THREAT DETECTED

Higiene de autenticación de correo mejorable en Acme Industries.com, sin exposición crítica de suplantación.

WHAT CAN HAPPEN (TECHNICAL)

Margen de mejora en la configuración; el riesgo de suplantación directa del dominio es limitado con la política actual.

RECOMMENDED ACTION (TECHNICAL)

Completar la autenticación de correo (DKIM / MTA-STS) y endurecer la política.

INDIVIDUAL FINDINGS (1)

1 **El SPF de Acme Industries.com no termina en '-all' ni '~all' — política ambigua.** Confidence 85

Registro SPF actual: v=spf1 redirect=_sssh9fwyv.sdmarc.net. Sin un mecanismo 'all' restrictivo, los receptores no saben qué hacer con remitentes no listados.

TAILORED RECOMMENDATION

Plan de remediación para Acme Industries Corp (Acme Industries.com):
1. Cerrar el SPF de Acme Industries.com terminándolo en "-all" (hard fail). Registro actual: v=spf1 redirect=_sssh9fwyv.sdmarc.net

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
El SPF de Acme Industries.com no termina en '-all' ni '~all' — política ambigua.	DNS (consulta directa)	–

Overall confidence: **BAJA** Sources queried: **1**

KRI 4 Perimeter Security / EASM

4/100 LOW

FOR THE INVESTOR — PRE-CLOSE

Acme Industries Corp has 54 subdomains listed under its main domain, creating multiple potential entry points for attackers. Although there are no critical services exposed, this broad attack surface complicates security management and increases the risk of exploitation. If an attacker gains access, they could manipulate company operations or defraud customers, leading to significant financial losses. In the M&A context, such vulnerabilities could result in unforeseen costs and liabilities, similar to the issues faced by companies like Yahoo and Equifax post-breach. Addressing these risks is essential before finalizing the acquisition.

FINANCIAL IMPACT

€130k-2M. An attacker could impersonate the CFO and defraud clients through fraudulent invoices.

HOW TO FIX IT

Minimize the number of subdomains to only those necessary and remove test environments from the internet.

WHO	Mid-size cyber consultancy such as Optiv or NCC Group
HOW	1) Conduct an audit of all subdomains.,2) Identify and retain only essential subdomains.,3) Remove unnecessary or test environments from public access.,4) Implement ongoing monitoring for new subdomains.
WHEN	Before deal close
TIME	1 month
FIX COST	**€30k-80k**
DIFFICULTY	MEDIUM
SEVERITY	MEDIUM

TECHNICAL DETAIL — THREAT DETECTED

Sin servicios críticos expuestos en Acme Industries.com; superficie de ataque contenida.

WHAT CAN HAPPEN (TECHNICAL)

La exposición perimetral se limita a servicios web estándar. El riesgo principal es la extensión del inventario, que amplía la superficie a vigilar.

RECOMMENDED ACTION (TECHNICAL)

Reducir el inventario de subdominios al mínimo necesario y retirar de internet los entornos de test.

INDIVIDUAL FINDINGS (1)

1 **Superficie de ataque amplia: 54 subdominios de Acme Industries.com.** Confidence 85

Netlas inventaría 54 subdominios bajo Acme Industries.com. Cada subdominio es un punto de entrada potencial; un inventario tan amplio dificulta el control y suele incluir activos olvidados o sin mantenimiento.

TAILORED RECOMMENDATION

Plan de perímetro para Acme Industries Corp (Acme Industries.com):
1. Inventariar los 54 subdominios de Acme Industries.com, dar de baja los obsoletos y dejar expuestos solo los imprescindibles.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
Superficie de ataque amplia: 54 subdominios de Acme Industries.com.	Netlas.io	netlas.io/

Overall confidence: **MEDIA** Sources queried: **1**

KRI 5 Reputational & Sentiment

0/100 LOW

SITUATION

Acme Industries Corp tiene cobertura de prensa (21 artículos en 12 meses) sin señales de crisis reputacional.

RECOMMENDED ACTION (TECHNICAL)

Sin acción reputacional inmediata. Mantener monitorización de prensa hasta el cierre.

INDIVIDUAL FINDINGS (0)

No individual findings under this indicator.

TAILORED RECOMMENDATION

No se detectaron señales de crisis reputacional para Acme Industries Corp en la prensa global (GDELT, últimos 12 meses). Mantener la monitorización hasta el cierre de la operación.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
— queried, no findings in this run —	*GDELT*	*www.gdeltproject.org/*

Overall confidence: **MEDIA** Sources queried: **1**

KRI 6 Legal & Regulatory

0/100 LOW

SITUATION

Acme Industries Corp no figura en las listas de sanciones de la OFAC (OFAC SDN List + OFAC Consolidated List) consultadas a fecha del análisis.

RECOMMENDED ACTION (TECHNICAL)

Sin acción requerida en el cribado de sanciones OFAC.

INDIVIDUAL FINDINGS (0)

No individual findings under this indicator.

TAILORED RECOMMENDATION

Acme Industries Corp no aparece en las listas OFAC consultadas. Para una due diligence legal completa, ampliar el cribado a las listas de la UE y la ONU, y revisar la sección "Legal Proceedings" del último 10-K para litigios y acciones regulatorias materiales.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
— queried, no findings in this run —	***OFAC SDN List***	–
— queried, no findings in this run —	***OFAC Consolidated List***	–

Overall confidence: **ALTA** Sources queried: **2**

KRI 7 Supply Chain Risk

16/100 LOW

FOR THE INVESTOR — PRE-CLOSE

Acme Industries Corp is exposed to risks from a third-party technology provider identified in its supply chain. If this vendor suffers a security incident, Acme could inherit vulnerabilities that lead to unauthorized access to sensitive data or operational disruptions. This is particularly concerning in the current regulatory environment, where fines for data breaches can reach up to €20 million. The risk is confirmed as the company depends on a vendor that has known security issues. In the M&A context, addressing these vulnerabilities is critical to avoid potential liabilities post-acquisition, similar to the repercussions faced by companies like Marriott and Yahoo after their breaches.

FINANCIAL IMPACT	**€380k-20M. A breach in the supply chain could lead to significant fines and reputational damage.**

HOW TO FIX IT

Conduct a thorough audit of all critical third-party vendors and their security certifications.

WHO	Mid-size cyber consultancy such as Optiv or NCC Group.
HOW	1) Identify all critical vendors in the supply chain.,2) Review their security certifications and compliance.,3) Negotiate cybersecurity clauses in vendor contracts.,4) Implement ongoing monitoring of vendor security post-acquisition.
WHEN	Before deal close
TIME	1 month
FIX COST	**€30-80k**
DIFFICULTY	MEDIUM
SEVERITY	MEDIUM

TECHNICAL DETAIL — THREAT DETECTED

Acme Industries Corp depende de 1 proveedores tecnológicos de terceros — superficie de riesgo heredada.

WHAT CAN HAPPEN (TECHNICAL)

Cada proveedor SaaS, cloud o de seguridad es un punto de fallo que el comprador hereda. Un atacante puede pivotar hacia la empresa a través de un proveedor comprometido (ataque de cadena de suministro), y una brecha en cualquiera de ellos expone datos del objetivo. El 60% de las brechas se originan en un tercero — y se heredan con la adquisición.

RECOMMENDED ACTION (TECHNICAL)

Inventariar los proveedores críticos, revisar sus certificaciones de seguridad y exigir cláusulas de ciberseguridad en sus contratos antes del cierre.

INDIVIDUAL FINDINGS (1)

1 **1 proveedores tecnológicos de terceros identificados en la cadena de suministro de Acme Industries Corp.** Confidence 80

Mediante señales DNS/HTTP públicas se identifican 1 proveedores de terceros de los que depende Acme Industries.com: Email / Workspace (Microsoft 365). Cada proveedor es una dependencia cuya seguridad el comprador hereda — el 60% de las brechas se originan en un tercero.

TAILORED RECOMMENDATION

Cadena de suministro de Acme Industries Corp (Acme Industries.com):
1. Proveedores de terceros identificados: Microsoft 365 [Email / Workspace].
2. Para cada proveedor crítico (cloud, email, identidad/SSO): solicitar sus informes de seguridad (SOC 2 / ISO 27001) y verificar su historial de brechas.
3. Revisar los contratos para confirmar cláusulas de notificación de incidentes y responsabilidad — el comprador hereda este riesgo.
4. Para un scoring de riesgo por proveedor (brechas conocidas, rating de seguridad), activar un feed dedicado de supply-chain risk.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
1 proveedores tecnológicos de terceros identificados en la cadena de suministro de Acme Industries Corp.	DNS / HTTP (consulta directa)	–
— queried, no findings in this run —	*DNS / HTTP*	*www.iana.org/*

Overall confidence: **MEDIA** Sources queried: **1**

KRI 8

Malicious Infrastructure / Typosquatting

35/100 MEDIUM

FOR THE INVESTOR — PRE-CLOSE

The presence of multiple lookalike domains registered by third parties poses a medium risk to Acme Industries. These domains could be used to impersonate the company, leading to fraudulent activities such as tricking clients into paying fake invoices. If exploited, this could result in significant financial losses and reputational damage. The risk is particularly relevant in the context of M&A, as unresolved issues could lead to increased liabilities post-acquisition. Similar cases, such as the impersonation incidents faced by other companies, highlight the potential for substantial financial repercussions.

FINANCIAL IMPACT **€130k-2M. An attacker could impersonate the company to defraud clients or siphon funds.**

HOW TO FIX IT

Conduct a thorough audit of the registered domains and take defensive actions.

WHO	Mid-size cyber consultancy such as Optiv or NCC Group.
HOW	1) Verify domain ownership through WHOIS lookup.,2) Monitor the identified domains for suspicious activity.,3) Register critical variations of the domain defensively.,4) Implement brand protection measures.
WHEN	Before deal close.
TIME	1 month
FIX COST	**€30-80k**
DIFFICULTY	MEDIUM
SEVERITY	MEDIUM

TECHNICAL DETAIL — THREAT DETECTED

9 dominios parecidos a Acme Industries.com están registrados por terceros; 1 con servidor de correo — vector latente de phishing.

WHAT CAN HAPPEN (TECHNICAL)

Estos dominios lookalike pueden activarse en cualquier momento para enviar correo casi idéntico al de la empresa o alojar páginas falsas. Es exposición latente: el atacante ya tiene la infraestructura, falta solo que la use.

RECOMMENDED ACTION (TECHNICAL)

Verificar por WHOIS la titularidad, monitorizar los dominios y registrar defensivamente las variantes críticas que sigan libres.

INDIVIDUAL FINDINGS (9)

1 Dominio similar registrado: antheus.com — con web activa

Confidence 88

antheus.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: GoDaddy.com, LLC.

2 Dominio similar registrado: latheus.com — con servidor de correo activo

Confidence 88

latheus.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: NameCheap, Inc.. Tiene servidor de correo — capaz de suplantar a la empresa por email.

3 Dominio similar registrado: Acme.com — con web activa

Confidence 88

Acme.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: TurnCommerce, Inc. DBA NameBright.com.

4 Dominio similar registrado: Acme.com — con web activa

Confidence 88

Acme.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Wild West Domains, LLC.

5 Dominio similar registrado: pantheus.com — con web activa

Confidence 88

pantheus.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: NameSilo, LLC.

6 Dominio similar registrado: Acme Industries.net — con web activa

Confidence 88

Acme Industries.net es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

7 Dominio similar registrado: Acme Industries.org — con web activa

Confidence 88

Acme Industries.org es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

8 Dominio similar registrado: Acme Industries.biz — con web activa

Confidence 88

Acme Industries.biz es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

9 Dominio similar registrado: Acme Industries.info — con web activa

Confidence 88

Acme Industries.info es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

TAILORED RECOMMENDATION

Plan de typosquatting para Acme Industries Corp (Acme Industries.com):
1. Dominios con servidor de correo capaces de suplantar a Acme Industries Corp: latheus.com. Verificar su titularidad por WHOIS; los que no sean defensivos, vigilar y solicitar takedown si se activan.
2. Vigilar estos dominios lookalike registrados (sin correo aún): antheus.com, Acme.com, Acme.com, pantheus.com, Acme Industries.net, Acme Industries.org, Acme Industries.biz, Acme Industries.info.
3. Nota: la confirmación de uso malicioso activo requiere activar una clave de URLhaus/abuse.ch (gratuita) — recomendado para distinguir amenaza activa de exposición latente.
4. Registrar defensivamente las variantes tipográficas críticas de Acme Industries.com que sigan libres y activar monitorización continua.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
Dominio similar registrado: antheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: latheus.com — con servidor de correo activo	DNS (consulta directa)	–
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: pantheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.net — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.org — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.biz — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.info — con web activa	DNS (consulta directa)	–
— queried, no findings in this run —	*RDAP*	*about.rdap.org/*

Overall confidence: **MEDIA** Sources queried: **2**

KRI 9 Shadow IT / Code Leaks

0/100 LOW

SITUATION

No se detectaron ficheros que expongan Acme Industries.com en contextos de secreto (.env, credenciales) en GitHub.

RECOMMENDED ACTION (TECHNICAL)

Sin acción inmediata. Mantener vigilancia de repositorios públicos.

INDIVIDUAL FINDINGS (0)

No individual findings under this indicator.

TAILORED RECOMMENDATION

No se hallaron secretos del dominio Acme Industries.com en contextos de riesgo en GitHub a fecha del análisis. Recomendado ampliar la vigilancia continua a GitLab y Pastebin. Ausencia de evidencia no equivale a evidencia de ausencia.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
— queried, no findings in this run —	*GitHub Code Search*	*github.com/search*

Overall confidence: **MEDIA** Sources queried: **1**

KRI 10 Dark Web Intelligence

18/100 LOW

FOR THE INVESTOR — PRE-CLOSE

Acme Industries is facing a confirmed risk as data associated with its domain is circulating on criminal forums, specifically in the form of logs that could facilitate unauthorized access. This exposure increases the likelihood of an attack that could lock the company's systems and demand a ransom, potentially costing between €1M and €3M in damages. The presence of these logs suggests that attackers could exploit this information to disrupt operations or defraud customers. In the M&A context, such vulnerabilities could lead to significant financial losses and reputational damage, similar to incidents faced by companies like Target and Equifax. Addressing this issue is critical to safeguarding the investment.

FINANCIAL IMPACT **€1-3M. An attacker could lock up the company's systems and demand a ransom.**

HOW TO FIX IT

Conduct a thorough investigation and implement protective measures against potential cyber threats.

WHO	Mid-size cyber consultancy such as Optiv or NCC Group.
HOW	1) Perform a dark web intelligence audit.,2) Identify and secure compromised accounts.,3) Implement enhanced monitoring for suspicious activities.,4) Train staff on cybersecurity awareness.
WHEN	Before deal close.
TIME	1 month
FIX COST	**€30-80k**
DIFFICULTY	MEDIUM
SEVERITY	MEDIUM

TECHNICAL DETAIL — THREAT DETECTED

Datos asociados a Acme Industries Corp circulan en canales de cibercrimen.

WHAT CAN HAPPEN (TECHNICAL)

Datos relacionados con la empresa circulan en canales de cibercrimen, sin credenciales de empleados entre ellos. Riesgo de dark web contenido según la cobertura disponible.

RECOMMENDED ACTION (TECHNICAL)

Vigilar los canales de cibercrimen y, para una due diligence M&A completa, activar un feed de inteligencia de dark web de pago.

INDIVIDUAL FINDINGS (1)

1 **Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).** Confidence 60

HudsonRock —fuente de inteligencia de cibercrimen— detecta 5 registro(s) de stealer logs asociados a Acme Industries.com (0 de empleados, 3 de usuarios, 2 de terceros). Los stealer logs son la mercancía principal de los mercados de dark web: estas credenciales y sesiones son comprables por un atacante.

TAILORED RECOMMENDATION

Inteligencia de dark web para Acme Industries Corp (Acme Industries.com):
1. Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).
2. Vigilar la evolución de la exposición en los próximos meses.
3. Cobertura parcial: la inteligencia profunda de dark web (foros cerrados de Initial Access Brokers, listados "access for sale") requiere activar un feed de pago. Activarlo es necesario para cubrir los listados "access for sale" de los foros cerrados — el indicador de mayor valor de este KRI en M&A.

VERIFIABLE SOURCES FOR THIS INDICATOR

FINDING / QUERY	SOURCE	VERIFIABLE AT
Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).	HudsonRock Cavalier	www.hudsonrock.com/

Overall confidence: **BAJA** Sources queried: **1**

CORPORATE GROUP

Corporate group & related entities (FLAGS)

This analysis is **entity-centric**, not just domain-centric. The entities listed here are **FLAGS for the acquirer to decide** whether to expand the engagement scope — they are **not verdicts about them**. Breach or dark-web exposure of a sibling company is NOT covered by a single-domain analysis; that is why we flag them.

No group entities were discovered via the automated keyless sources (GLEIF, OpenCorporates, WhoXY, shared infrastructure) for this company.

GROUP-DISCOVERY SOURCE STATUS

—

> Honest scope note: group discovery here comes from official relationships (GLEIF), corporate registries (OpenCorporates), reverse-WHOIS (WhoXY) and shared infrastructure. **Exhaustive** group discovery via web/LinkedIn search (trading brands and affiliates these sources do not register) requires the search-engine phase (pending) or analyst input. The absence of entities here does NOT mean the group does not exist.

VERIFIABLE SOURCES

Full traceability

Every finding in this report comes from a **verifiable public source**. This section lists every URL and source queried, grouped by KRI. **Don't take our word — verify.** If a URL stops responding in the future, we retain a snapshot taken at analysis time with an RFC 3161 timestamp, available on request.

1 Executive Digital Exposure

1 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
Gobierno corporativo de Acme Industries Corp públicamente identificado: 18 personas (7 con cargo ejecutivo, 10 consejeros).	SEC EDGAR (Forms 3/4)	www.sec.gov/

2 Known Breaches & Credentials

2 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
3 usuario(s) de aplicaciones de Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/
2 tercero(s) con acceso relacionado con Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/

3 DNS Weaknesses & Hygiene

1 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
El SPF de Acme Industries.com no termina en '-all' ni '~all' — política ambigua.	DNS (consulta directa)	–

4 Perimeter Security / EASM

1 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
Superficie de ataque amplia: 54 subdominios de Acme Industries.com.	Netlas.io	netlas.io/

5 Reputational & Sentiment

0 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
— queried, no findings in this run —	*GDELT*	*www.gdeltproject.org/*

6 Legal & Regulatory

0 findings · 2 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
— queried, no findings in this run —	*OFAC SDN List*	–
— queried, no findings in this run —	*OFAC Consolidated List*	–

7 Supply Chain Risk

1 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
1 proveedores tecnológicos de terceros identificados en la cadena de suministro de Acme Industries Corp.	DNS / HTTP (consulta directa)	–
— queried, no findings in this run —	*DNS / HTTP*	*www.iana.org/*

8 Malicious Infrastructure / Typosquatting

9 findings · 2 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
Dominio similar registrado: antheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: latheus.com — con servidor de correo activo	DNS (consulta directa)	–
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: pantheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.net — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.org — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.biz — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.info — con web activa	DNS (consulta directa)	–
— queried, no findings in this run —	*RDAP*	*about.rdap.org/*

9 Shadow IT / Code Leaks

0 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
— queried, no findings in this run —	*GitHub Code Search*	*github.com/search*

10 Dark Web Intelligence

1 findings · 1 sources queried

FINDING / QUERY	SOURCE	VERIFIABLE AT
Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).	HudsonRock Cavalier	www.hudsonrock.com/

SCOPE PER INDICATOR

Scope & queries per indicator

Full method transparency: for each KRI, the **literal** query or dork we executed. So you know exactly what was searched and how far each indicator reaches — we don't ask you to blindly trust a colour label.

1 Executive Digital Exposure

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

2 Known Breaches & Credentials

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

3 DNS Weaknesses & Hygiene

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

4 Perimeter Security / EASM

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

5 Reputational & Sentiment

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

6 Legal & Regulatory

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

7 Supply Chain Risk

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

8 Malicious Infrastructure / Typosquatting

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

9 Shadow IT / Code Leaks

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

10 Dark Web Intelligence

WHAT WE LOOKED FOR	QUERY EXECUTED	LIMIT
No queries recorded for this indicator in this run.		

METHODOLOGY AND LEGAL NOTICE

How we work and why this report is defensible

INFORMATION ORIGIN — PUBLIC SOURCES ONLY (OSINT)

All content in this report comes from **publicly available information** (Open Source Intelligence). At no point were the target company's systems accessed, no intrusive action was taken and no unauthorized credentials were used. Sources queried include official company registries (SEC EDGAR, BORME, Companies House, GLEIF), international sanctions lists (OFAC, United Nations, UK HMT/OFSI), public databases of historical security breaches (HudsonRock, Have I Been Pwned, LeakCheck), global press indexes (Event Registry, NewsData, Google News), exposed-infrastructure search engines (Shodan, Censys, Netlas), threat-intelligence aggregators (AbuseIPDB, GreyNoise, VirusTotal, AlienVault OTX) and Tor-network search engines (Ahmia). The complete, verifiable list of every source, grouped by indicator, is provided in the "Verifiable Sources" section of this report.

LEGAL BASIS OF THE ANALYSIS

This report is prepared under the **legitimate interest of the requester** (Article 6.1.f of the EU General Data Protection Regulation 2016/679, GDPR) in the evaluation, prior to or alongside a merger, acquisition, investment or contractual relationship with the target company. The primary subject of the analysis is a legal entity, not sensitive personal data. Personally identifiable information that appears (typically professional data of executives in official company registries or historical public leaks) is included solely where necessary to assess the risk that is the subject of the report, in line with the data-minimization principle of Article 5.1.c GDPR. The requester bears final responsibility for use of the report within a legitimate, authorized corporate due-diligence context.

EVIDENTIARY CUSTODY — RFC 3161

The content of this report is sealed with a **cryptographic timestamp compliant with the RFC 3161 standard**, issued by a Time-Stamping Authority (TSA) at the exact moment of generation. The seal demonstrates, in a technically verifiable way, that the content described here existed at the stated date and time and has not been altered since. Independent verification can be performed with any RFC 3161-compatible tool (for example, `openssl ts -verify`). The seal file (`.tsr`) is available on request. Note: FreeTSA is not an eIDAS Qualified Trust Service Provider; for full qualified evidentiary validity (eIDAS Art. 42) migration to an eIDAS QTSP is required. Discuss with the requester if this migration is needed.

REQUESTER RETENTION AND PRIVACY

The report is stored on IntelMind's systems for **30 calendar days** from issuance, accessible solely to the user who requested it from their private panel, to allow reprints and later consultation. After that period the PDF and analytical content are automatically deleted; only the RFC 3161 custody seal (which contains no personal data, just a hash) is retained for the applicable legal term, for future evidentiary verification. The requester may request immediate deletion of the report at any time by contacting soporte@intelmind.io. An "**ephemeral delivery**" mode is also available: the PDF is sent to the requester's email without being stored on IntelMind's systems (only the custody seal is retained). This option is activated at purchase, at no extra cost.

HONEST LIMITATIONS OF THE ANALYSIS

- El informe refleja lo hallado en fuentes públicas dentro de la ventana de análisis. La ausencia de evidencia no equivale a evidencia de ausencia.
- Cada hallazgo es válido a la fecha y hora del escaneo.
- Las coincidencias por nombre (sanciones, dominios similares) requieren verificación de identidad antes de darse por confirmadas.
- Algunos indicadores entregan una evaluación parcial; su profundidad máxima requiere feeds de inteligencia de pago, indicado en cada caso.

PROFESSIONAL DISCLAIMER

This report constitutes a technical-informational analysis prepared by IntelMind using an outside-in methodology. It does not replace the legal, tax, financial or specialized audit advice that the requester should obtain. Remediation recommendations and economic benchmarks are provided as guidance and must be validated case by case with the relevant advisors. IntelMind does not guarantee the absolute accuracy of information obtained from public third-party sources, although it applies the disciplined cross-verification controls described in this section. Use of the report is subject to the terms and conditions published at intelmind.io.

PUBLIC VERIFICATION OF THE SEAL

The integrity of this document can be verified at `https://intelmind.io/cyber-dd/verify/IMD-CDF-MU8KBTND-YUDF` at any future time, while the custody period remains valid.