
SKURIO
TAILOR YOUR CYBER THREAT INTELLIGENCE
JEREMY HENDY, CEO
COMMERCIAL IN CONFIDENCE

TAILOR YOUR THREAT INTELLIGENCE

NEW UPDATES TO ISO27001 AND ISO27002


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

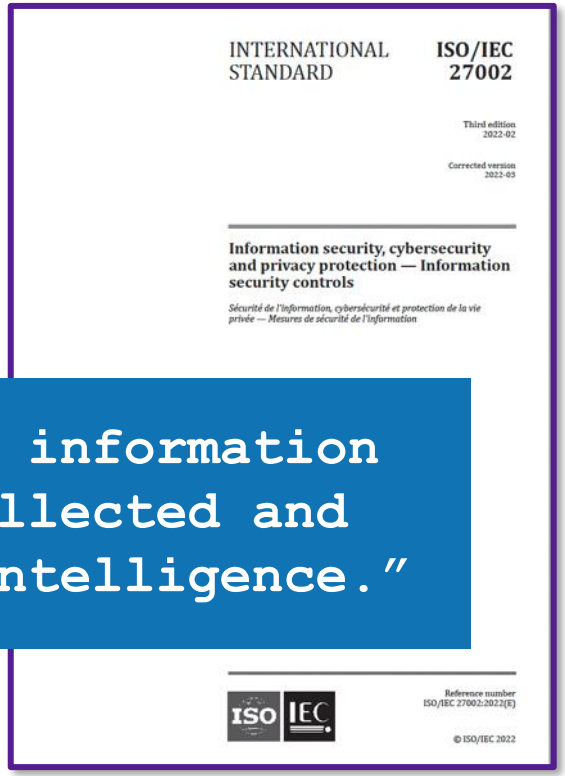
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

- First update since 2013
- 11 new security controls
- Summary in ISO27001
- Detail in ISO27002


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Corrected version
2022-03

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

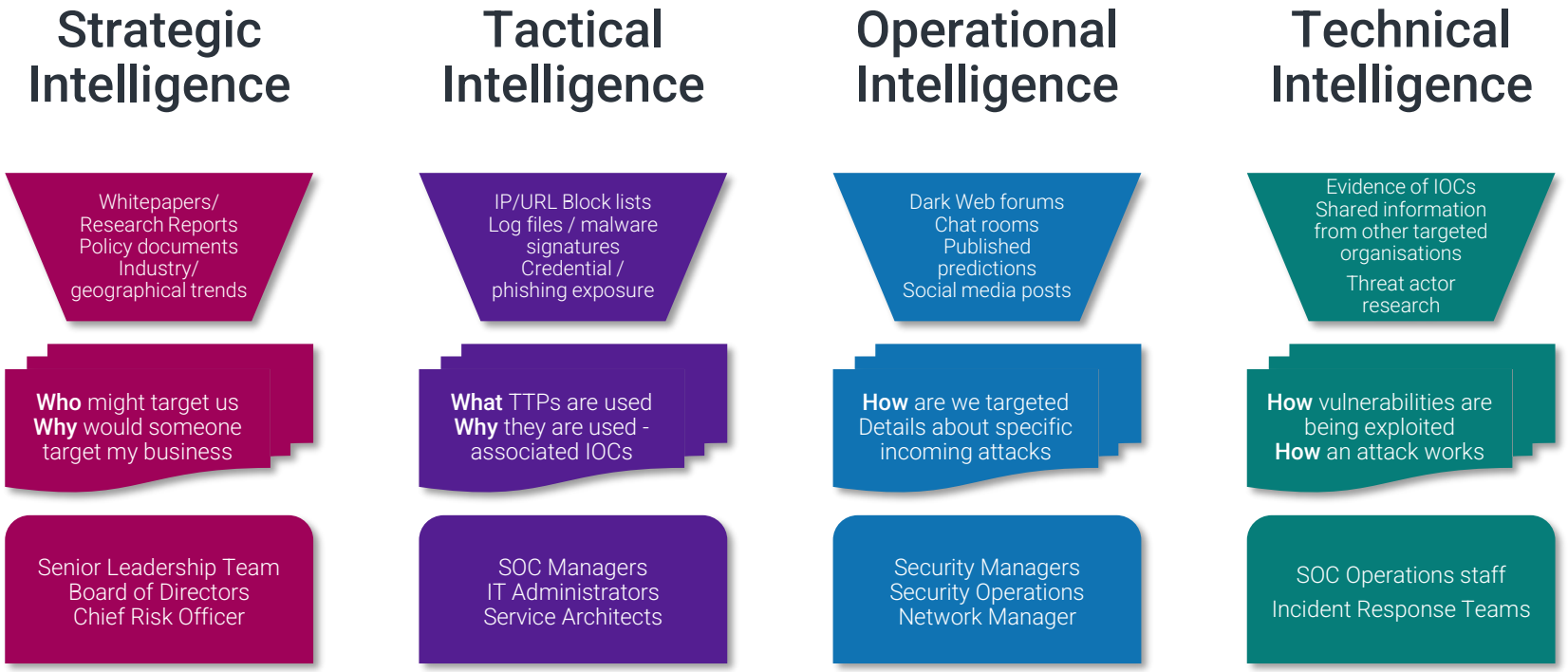
Reference number
ISO/IEC 27002:2022(E)

© ISO/IEC 2022

5.7 "Information relating to information security threats shall be collected and analysed to produce threat intelligence."

"Threat intelligence is data that is collected, processed, and analysed to understand a threat actor's motives, targets, and attack behaviours"

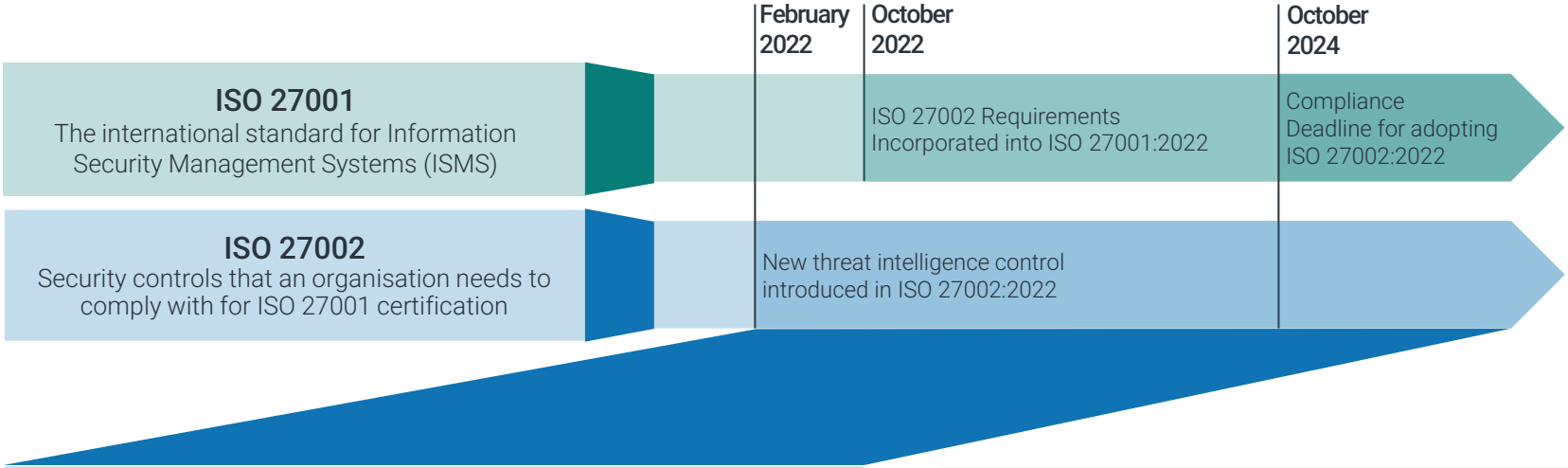
FOUR TYPES OF CYBER THREAT INTELLIGENCE



TTPs - Tactics, Techniques and Procedures
IOCs - Indicators for compromise

SKURIO

ISO 27001 CHANGES



New controls added

5.7	Threat intelligence	8.10	Information deletion
5.23	Information security for use of cloud services	8.11	Data masking
5.30	ICT readiness for business continuity	8.12	Data leakage prevention
7.4	Physical security monitoring	8.16	Monitoring activities
8.9	Configuration management	8.23	Web filtering
		8.28	Secure coding

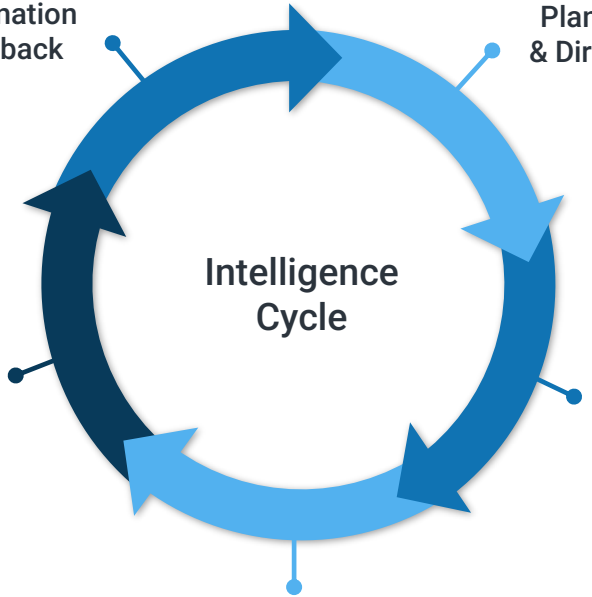
Controls have 5 types of attributes

Control type (preventive, detective, corrective)
Information security properties (confidentiality, integrity, availability)
Cybersecurity concepts (identify, protect, detect, respond, recover)
Operational capabilities (governance, asset management, etc.)
Security domains (governance & ecosystem, protection, defense, resilience)

ISO27002:2022 GUIDANCE FOR THREAT INTELLIGENCE

Relevant	Insightful	Contextual	Actionable
Does this relate to my organisation?	Accurate	Where?	Quickly
	Detailed	When?	Effectively

REQUIREMENTS MAP TO THE INTELLIGENCE CYCLE



Step 1 : Planning & Direction

"Establishing objectives for threat intelligence production"

Step 2 : Data Collection

"Identifying & selecting information sources that are necessary and appropriate"

Step 3 : Data Processing

"Collecting information from selected sources"

Step 4 : Analysis & Production

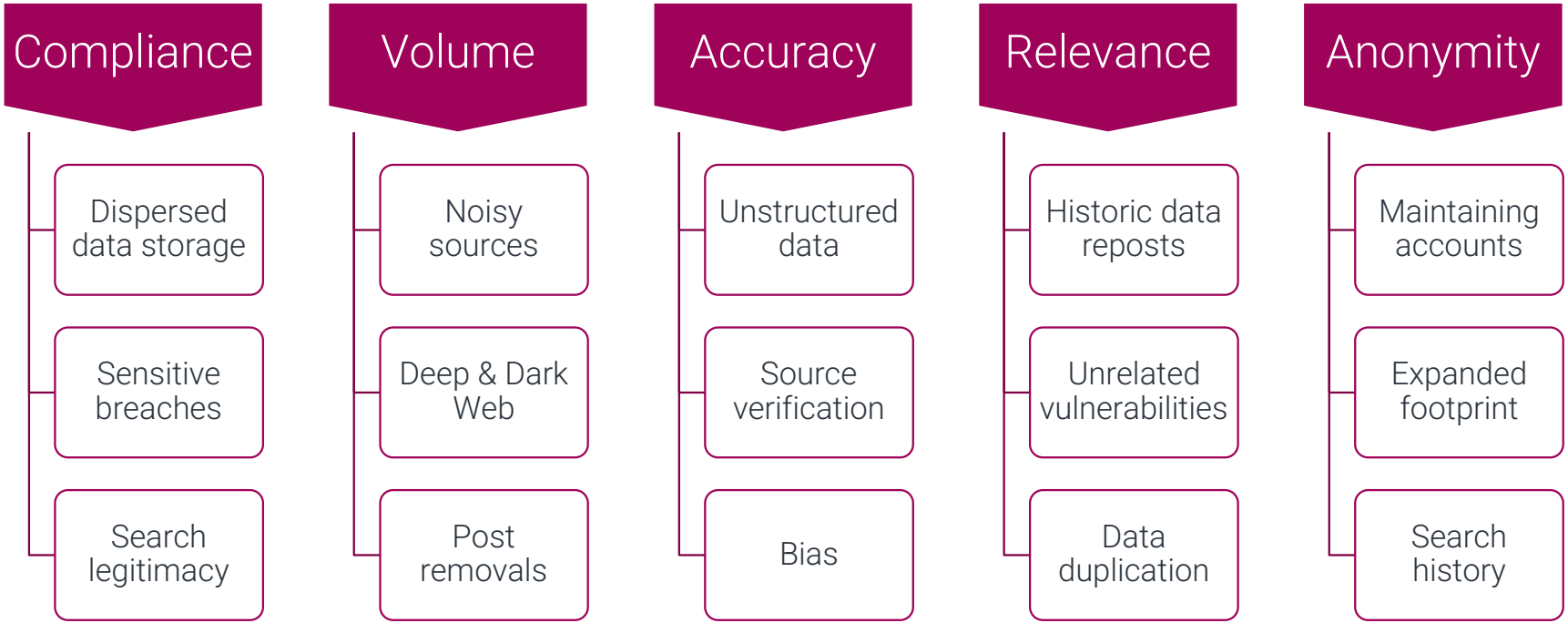
"Processing information to prepare it for analysis"

Step 5 : Dissemination & Feedback

"Analysing information to understand how it relates and is meaningful to the organisation"

"Communicating and sharing it to relevant individuals in a format that can be understood"

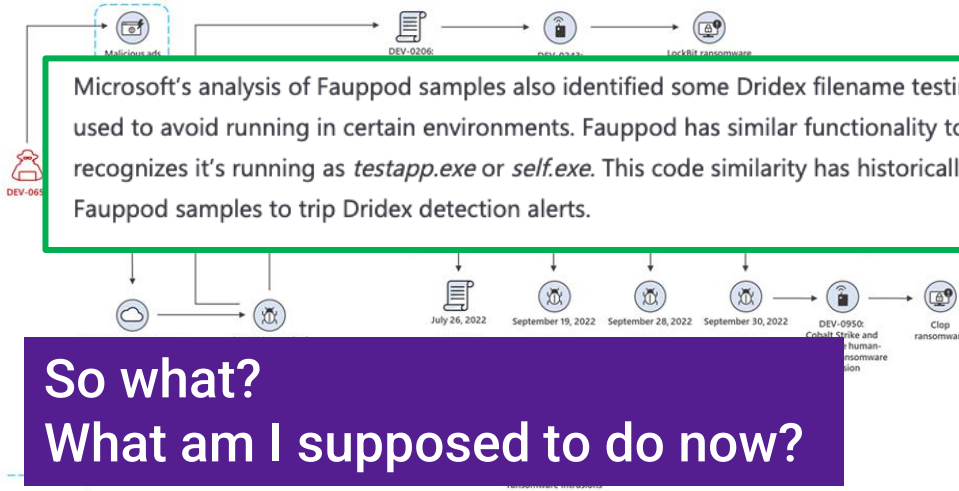
THE THREAT INTELLIGENCE CHALLENGE



October 27, 2022 • 15 min read

Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity

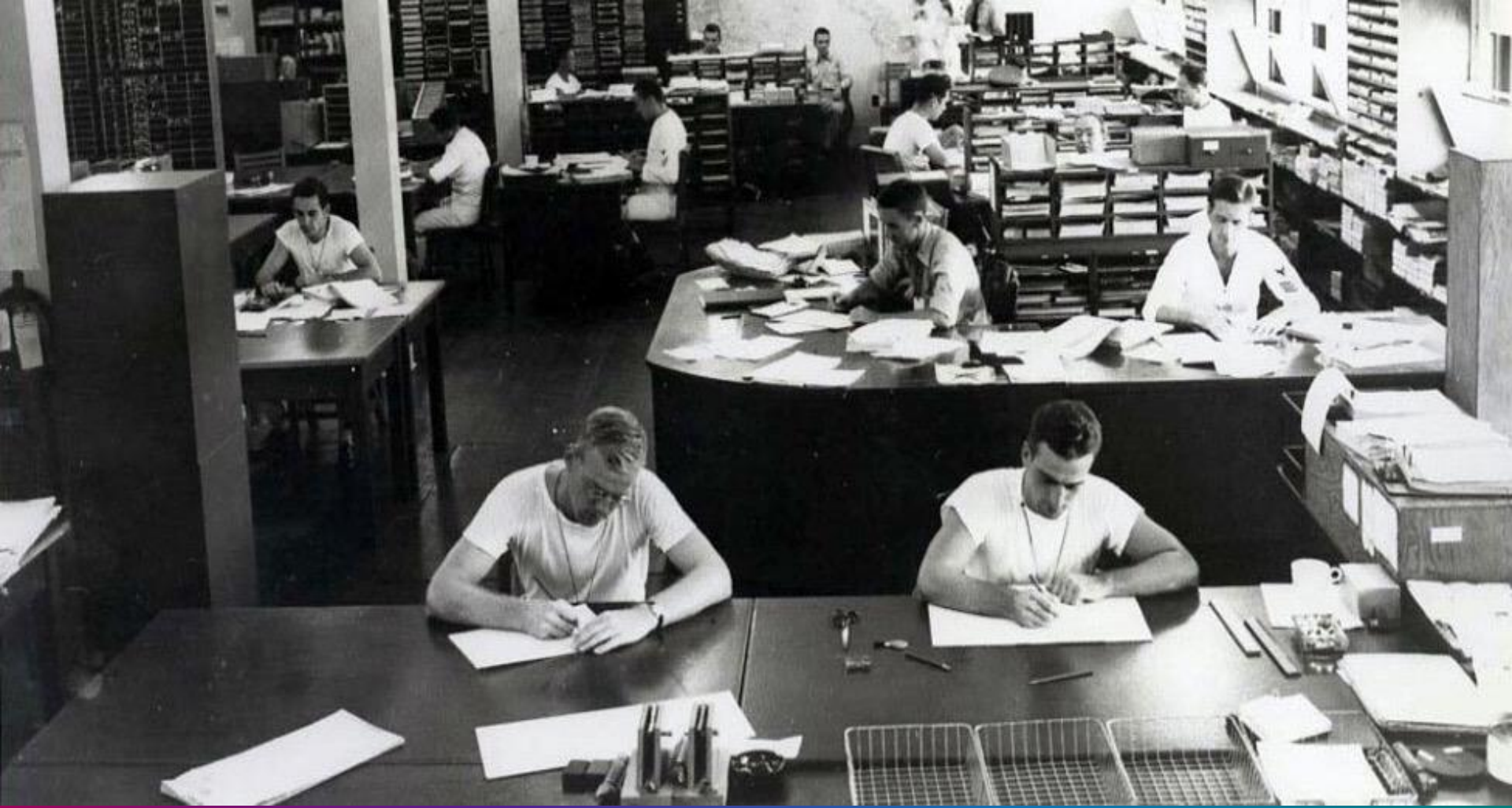
Microsoft Security Threat Intelligence



Microsoft's analysis of Fauppod samples also identified some Dridex filename testing features, which are used to avoid running in certain environments. Fauppod has similar functionality to avoid execution if it recognizes it's running as *testapp.exe* or *self.exe*. This code similarity has historically caused some Fauppod samples to trip Dridex detection alerts.

So what?
What am I supposed to do now?

```
text:00401010                   sub_401010      proc near               ; CODE XREF: DllEntryPoint:loc_4010D14p
text:00401010
text:00401010                   var_D           = byte ptr -0Dh
text:00401010                   var_C           = dword ptr -0Ch
text:00401010                   var_8           = dword ptr -8
text:00401010                   var_4           = dword ptr -4
text:00401010
text:00401010 55                                push    ebp
text:00401011 89 E5                             mov     ebp, esp
text:00401013 83 EC 14                          sub     esp, 14h
text:00401016 31 C0                             xor     eax, eax
text:00401018 8B 0D A0 30 40 00                 mov     ecx, ds:CloseHandle
text:0040101E 80 39 B8                          cmp     byte ptr [ecx], 0B8h
text:00401021 89 45 FC                          mov     [ebp+var_4], eax
text:00401024 74 1D                             jz      short loc_401043
text:00401026 A1 A4 30 40 00                    mov     eax, ds:GetCurrentThreadId
text:0040102B FF D0                             call    eax ; GetCurrentThreadId
text:0040102D B9 01 00 00 00                    mov     ecx, 1
text:00401032 8B 15 A8 30 40 00                 mov     edx, ds:OutputDebugStringA
text:00401038 80 3A 6A                          cmp     byte ptr [edx], 6Ah
text:0040103B 89 45 F8                          mov     [ebp+var_8], eax
text:0040103E 89 4D FC                          mov     [ebp+var_4], ecx
text:00401041 75 38                             jnz     short loc_40107B
text:00401043
text:00401043                   loc_401043:                             ; CODE XREF: sub_401010+14↑j
text:00401043                                                           ; sub_401010+5A↓j ...
text:00401043 8B 45 FC                          mov     eax, [ebp+var_4]
text:00401046 83 C4 14                          add     esp, 14h
text:00401049 5D                                pop     ebp
text:0040104A C3                                retn
text:0040104B                   ; ---------------------------------------------------------------------------
text:0040104B                   loc_40104B:                             ; CODE XREF: sub_401010+93↓j
text:0040104B                                   mov     eax, esp
text:0040104D                                   mov     dword ptr [eax], offset aSelfExe ; "self.exe"
text:00401053                                   mov     eax, ds:GetModuleHandleA
text:00401058                                   call    eax ; GetModuleHandleA
text:0040105A                                   sub     esp, 4
text:0040105D                                   mov     ecx, 1
text:00401062                                   cmp     eax, 0
text:00401065                                   mov     [ebp+var_4], ecx
text:00401068                                   jnz     short loc_401043
text:0040106A                                   call    sub_4017D0
text:0040106F                                   mov     [ebp+var_C], eax
text:00401072                                   xor     eax, eax
text:00401074 31 C0                             mov     [ebp+var_4], eax
text:00401076 89 45 FC                          jmp     short loc_401043
text:00401079 EB C8                             ; ---------------------------------------------------------------------------
text:0040107B
text:0040107B                   loc_40107B:                             ; CODE XREF: sub_401010+31↑j
text:0040107B 89 E0                             mov     eax, esp
text:0040107D C7 00 08 71 48 00                 mov     dword ptr [eax], offset aTestappExe ; "testapp.exe"
text:00401083 A1 B0 30 40 00                    mov     eax, ds:LoadLibraryW
text:00401088 FF D0                             call    eax ; LoadLibraryW
text:0040108A 83 EC 04                          sub     esp, 4
text:0040108D 3D 00 00 00 00                    cmp     eax, 0
text:00401092 0F 94 C1                          setz    cl
text:00401095 88 4D F3                          mov     [ebp+var_D], cl
text:00401098 31 C0                             xor     eax, eax
text:0040109A 8A 4D F3                          mov     cl, [ebp+var_D]
text:0040109D F6 C1 01                          test    cl, 1
text:004010A0 89 45 FC                          mov     [ebp+var_4], eax
text:004010A3 75 A6                             jnz     short loc_401048
text:004010A5 EB 9C                             jmp     short loc_401043
text:004010A5                   sub_401010      endp
```



How is tailored threat intelligence different?

SKURIO

SKURIO IS DIFFERENT TO TRADITIONAL THREAT INTELLIGENCE

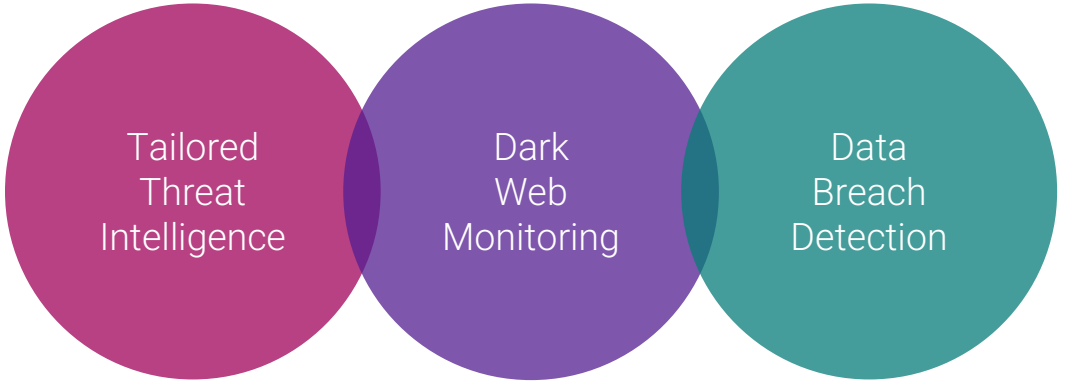
Traditional Cyber Threat Intelligence Providers	SKURIO
Generic Threat Intelligence	Tailored Threat Intelligence	Data Breach Detection
• Feeds of “bad stuff”, not specific to you • Malicious IP addresses • Malware signatures • Nation State / APT Activity • Exploits & Vulnerabilities	• Alerting you to threats specific to your organization • Credentials, Domains, Infrastructure, People, Assets, Sites, Intellectual Property…	• Detecting leaks of your data throughout the supply chain • Customer & Staff data, Intellectual Property, Business Critical Information

TAILORING YOUR THREAT INTELLIGENCE

Keep it relevant	Specific to you	Focus on core threats
Automate	SaaS applications	Orchestrated flows
Ease of Use	Configure in 30 minutes	Minimal ongoing resource

HOW DO WE DO THAT?

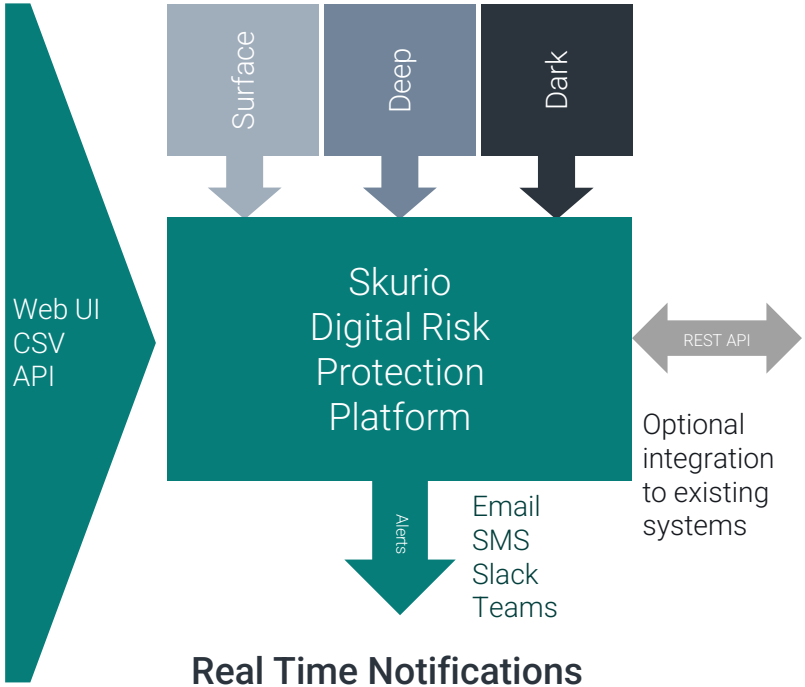
- Automated SaaS platform
- Looking “outside the firewall”
- Continuous, real-time monitoring
- SaaS only, or plus analyst services
- Detect leaks and breaches across your supply chain
- Protect your core assets



TAILORING YOUR THREAT INTELLIGENCE

Use cases	Search Terms (static or dynamic)	
Staff	Corporate domains VIP information	| Hashed email addresses | Banking details
Infrastructure	Server names IP addresses Device serial numbers	| Database table prefixes | IP Address ranges | Database table prefixes
Customers	Breachmarkers Postcodes	| Hashed email addresses | Reference numbers
Brand	Brand Names Company names Keywords	| Domains (typosquatting) | Product names
Margin	Discount codes Contract terms	| Loyalty scheme details | Voucher details
Products	Trademark details Product data Partner brands + IOCs	| Intellectual property terms | Code markers

Continuous, Automated Monitoring



Real Time Notifications

SKURIO - COMPANY OVERVIEW

- UK Cybersecurity company
  - Development & Operations: Belfast, Northern Ireland
  - Sales, Marketing, Finance, Customer Success: London
  - Intelligence Analysts: England & NI
- Operating since 2011
  - Original focus: UK government & public sector
  - Since 2017: refocus on the commercial sector
- What we do: Digital Risk Protection
  - Cloud-hosted SaaS platform
  - Dark Web monitoring
  - Data breach detection
  - Cyber threat intelligence

TECH NATION CYBER

NI CYBER
Northern Ireland Cyber Security Cluster

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ISO 27001 Certified

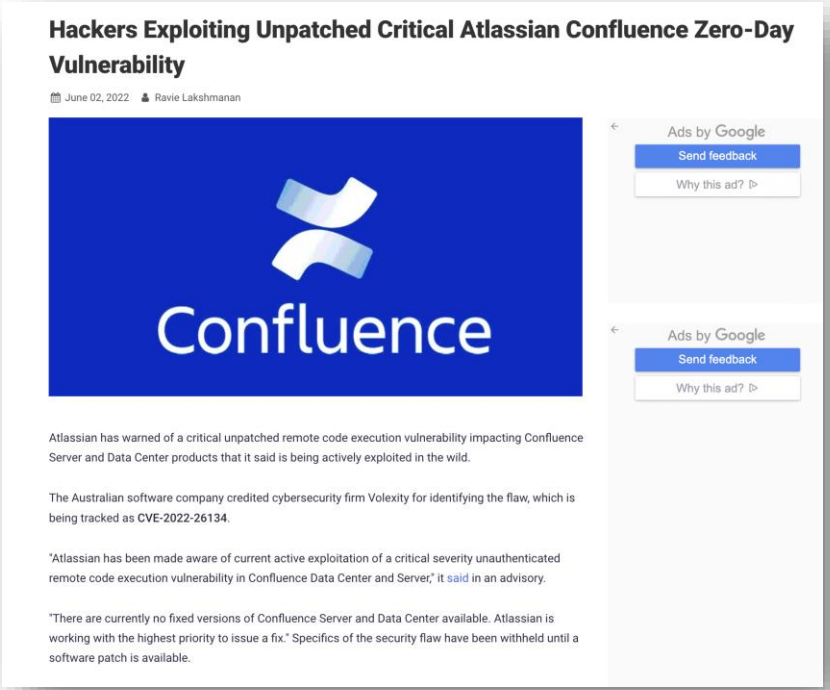
CYBER ESSENTIALS

DEMO & QUESTIONS?

- Discover DRP use cases
- Have a personalized view of Skurio in action
- Request a risk assessment

Examples

TESTING IF YOUR THREAT INTEL MEETS THE STANDARD



Hackers Exploiting Unpatched Critical Atlassian Confluence Zero-Day Vulnerability

June 02, 2022 Ravie Lakshmanan

Confluence

Ads by Google
Send feedback
Why this ad?

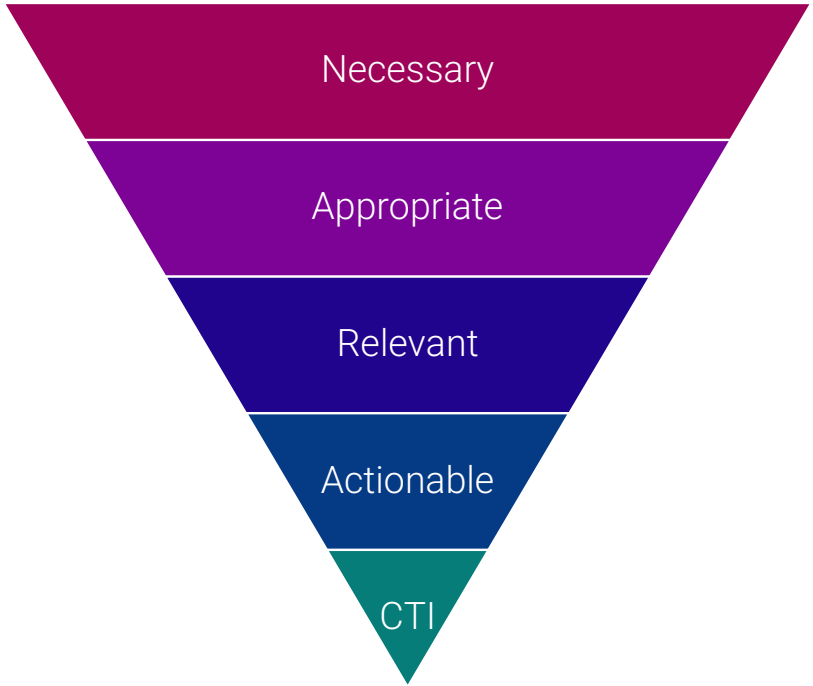
Ads by Google
Send feedback
Why this ad?

Atlassian has warned of a critical unpatched remote code execution vulnerability impacting Confluence Server and Data Center products that it said is being actively exploited in the wild.

The Australian software company credited cybersecurity firm Volexity for identifying the flaw, which is being tracked as **CVE-2022-26134**.

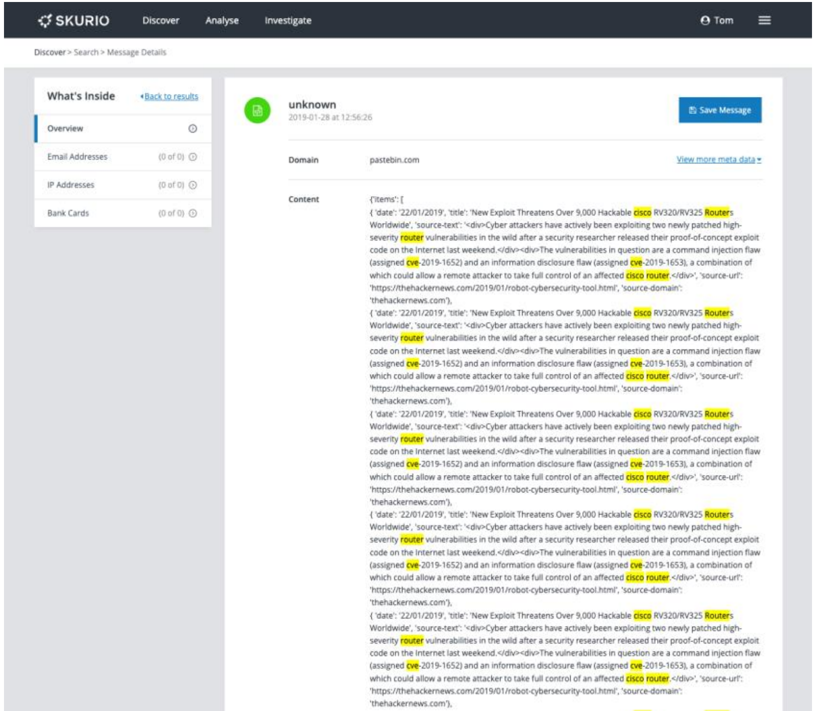
"Atlassian has been made aware of current active exploitation of a critical severity unauthenticated remote code execution vulnerability in Confluence Data Center and Server," it said in an advisory.

"There are currently no fixed versions of Confluence Server and Data Center available. Atlassian is working with the highest priority to issue a fix." Specifics of the security flaw have been withheld until a software patch is available.



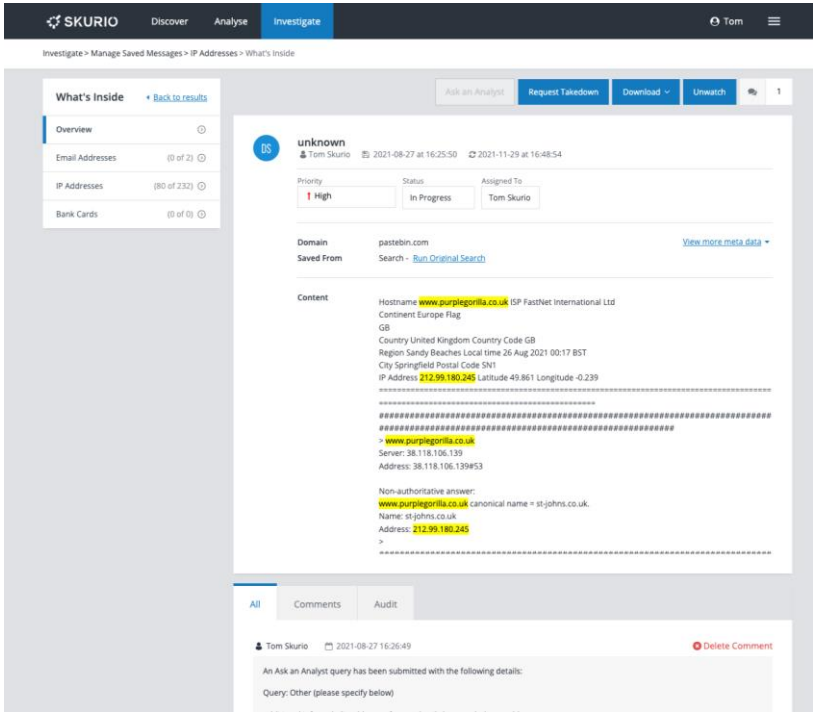
DRP EXAMPLE – SUPPLY CHAIN BREACH

- What are we looking for?
  - Equipment vulnerability
- How do we tailor the search?
  - Model number / range
- What results might we find?
  - Relevant CVEs / Zero Days
  - Stolen equipment
  - Default setting exposure
- What steps can be taken?
  - Patching / upgrades
  - Additional monitoring
  - Augment perimeter defences



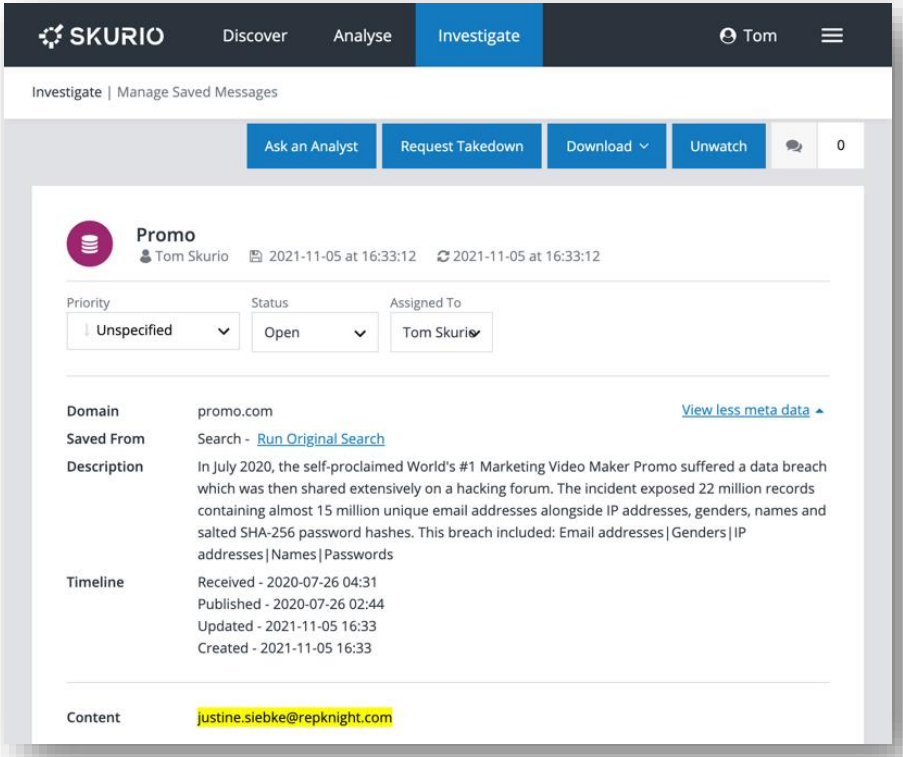
DRP EXAMPLE – INFRASTRUCTURE

- What are we looking for?
  - Mentions of our infrastructure terms
    - IP addresses etc.
- How do we tailor the search?
  - Individual IP addresses
  - Domain names
  - ‘Tailored IOCs’ e.g. “open port”, ”DDoS”
- What results might we find?
  - Evidence of recon
  - Possible attack planning
- What steps can be taken?
  - Proactive threat hunt searches
  - Beef up defences in specific areas
  - Patch / close ports etc.



DRP EXAMPLE – STAFF CREDENTIALS

- What are we looking for?
  - Data breaches
  - Spearphishing planning
- How do we tailor the search?
  - Key staff emails: admins / marketing / c-suite / finance
- What results might we find?
  - Unauthorised use of 3rd party apps
  - Password sharing
- What steps can be taken?
  - Application policy
  - Awareness training
  - Password refresh



DRP EXAMPLE – VIP PROTECTION

- What are we looking for?
  - PII
- How do we tailor the search?
  - Partial payment details
  - Mobile number / social media account mentions
- What results might we find?
  - Trolling
  - Doxxing
  - Evidence of whalephishing
  - Targeting family members
- What steps can be taken?
  - Patching / upgrades
  - Additional monitoring
  - Augment perimeter defences