Trellix

Operationalising Threat Intelligence

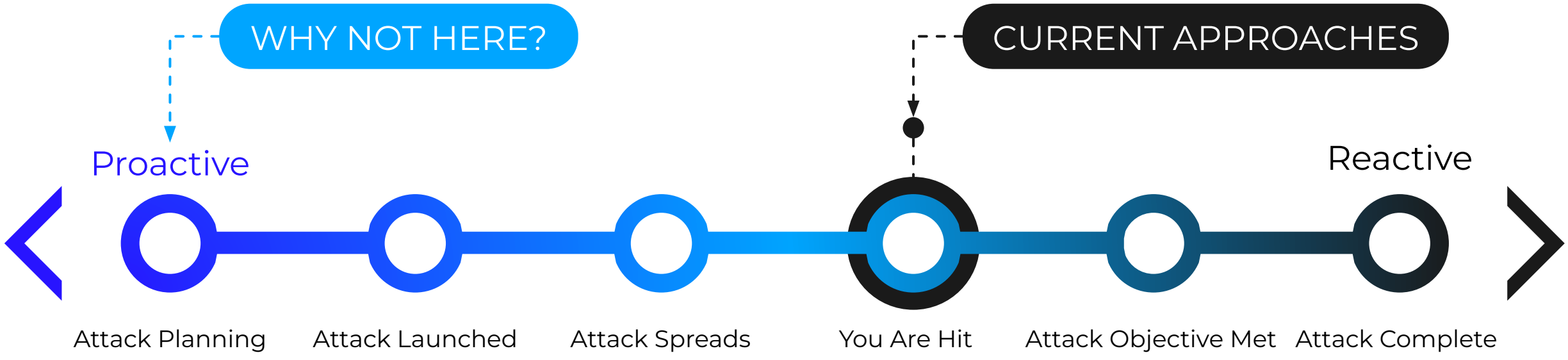
Outsmart Your Adversaries

James Murphy
Senior Threat Intelligence Architect

Bevan Read
Senior Threat Intelligence Consultant

July 11, 2024

Let's Get "Left of Boom"



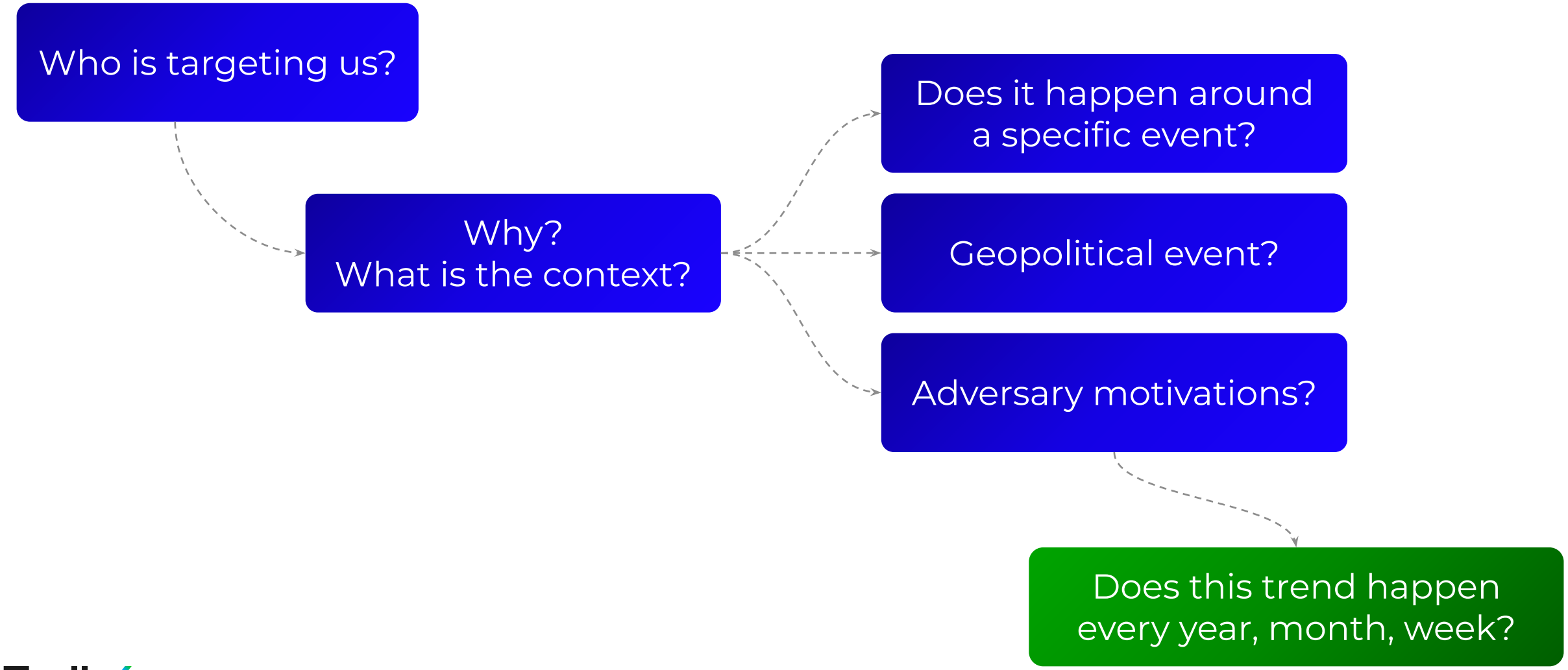
Trellix

> “Knowing who your adversary was told you what you needed to protect and how to defend yourself.”

Dmitri Alperovitch

Trellix

Who, Why, When?

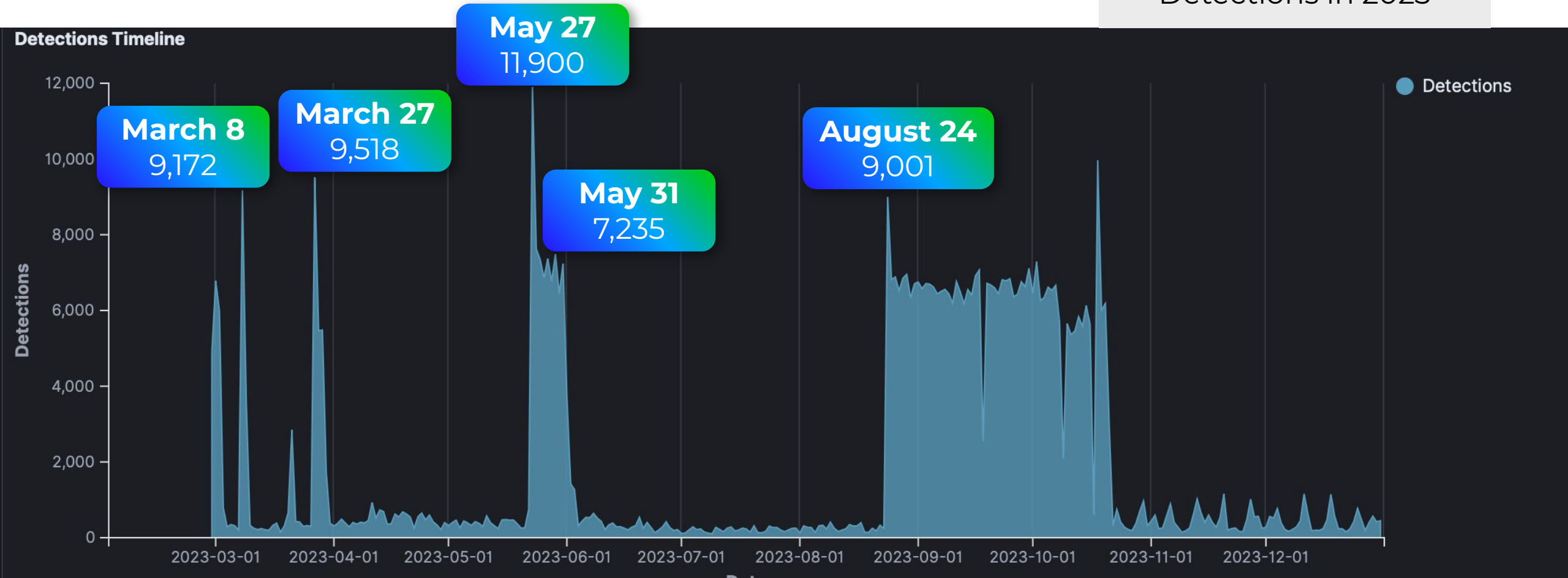


Trellix

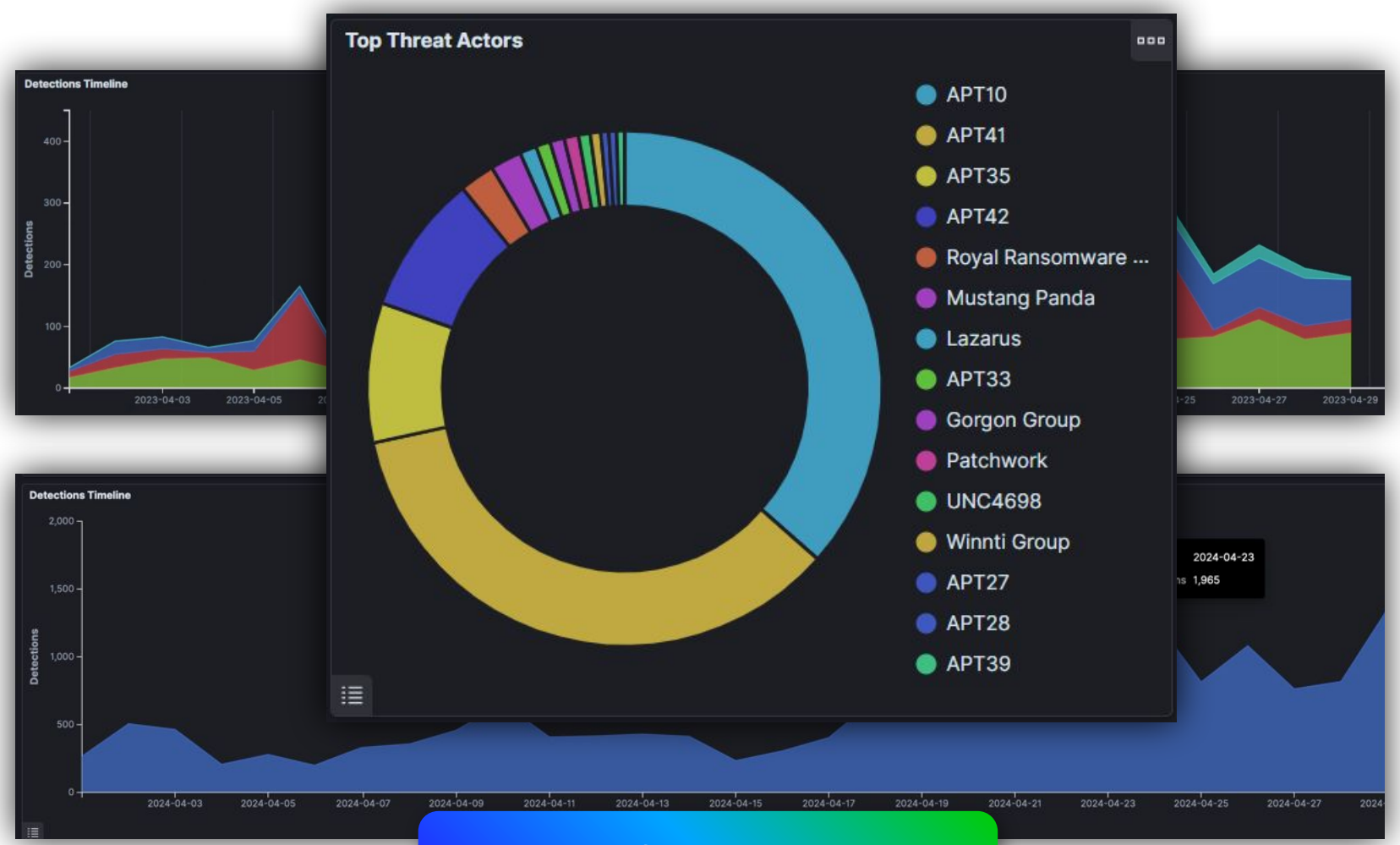
Connecting the Dots

North Korea-related cyber threat activity in 2023

Number of Malicious Detections in 2023



Connecting the Dots



ANZAC Day
April 25th 2023

ANZAC Day
April 25th 2024

Trellix ATLAS

Trellix

Quick Win for Operational Threat Intelligence

THREAT HUNT RULES

Yara Rules | Sigma Rules

Search Filters

Categories

- Payload delivery
- Payload installation
- Artifacts dropped

Payload delivery

```
rule Lockbit2_Jul21 {
   meta:
      description = "simple rule to detect latest Lockbit ransomware Jul 2021"
      author = "CB @ ATR"
      date = "2021-07-28"
      version = "v1"
      hash1 = "f32e9fb8b1ea73f0a71f3edaebb7f2b242e72d2a4826d6b2744ad3d830671202"
      hash2 = "dd8fe3966ab4d2d6215c63b3ac7abf4673d9c19f2d9f35a6bf247922c642ec2d"

   strings:
      $seq1 = " /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 \"%s\"
      $seq2 = "\"C:\\Windows\\system32\\mshta.exe\" \"%s\"" fullword wide
      $p1 = "C:\\windows\\system32\\%X%X%X.ico" fullword wide
      $p2 = "\\??\\C:\\windows\\system32\\%X%X%X.ico" fullword wide
      $p3 = "\\Registry\\Machine\\Software\\Classes\\Lockbit\\shell\\Open\\Command" fullword wide
      $p4 = "use ToxID: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7"
      $p5 = "https://tox.chat/download.html" fullword wide
      $p6 = "Software\\Microsoft\\Windows NT\\CurrentVersion\\ICM\\Calibration" fullword wide
      $p7 = "http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion" fullword wide
      $p8 = "\\LockBit_Ransomware.hta" fullword wide
```

MITRE ATT&CK EXPLORER

Reconnaissance | Lateral Movement | Collection

Active Scanning | Lateral Tool Transfer | Archive via | DNS | Exfiltration Over | Data Encrypted for Impact

Scan Database | Pass the | Resource Hijacking

Business Relationships | Remote Protocol | Account Access Removal

CDNs | SMB/Win Admin S | Application Exhaustion Flood

Client Configur | Application Token | Application or System Exploitation

Code Repositor | Distribute Compone | Data Destruction

Credentials | Exploitati Remote S | Data Manipulation

DNS | Internal Spearphis | Defacement

Tool

CrossWalk | PowerShell | FRP | FTP

ScrambleCross | Schtasks.exe | 7-Zip

nmap | Meterpreter | Reg | Systeminfo

Tasklist | netstat | ysoserial | OneForAll

Windows Service Configuration Tool | whoami

Living off the Land | ASPXSpy | Mimikatz

Subdomain3 | Esentutl | ZXShell

StealthMutant | Icacls | VSSAdmin

Cobalt Strike | JexBoss | BadPotato

pwdump | BITSAdmin | Ping.exe | Sublist3r

Net | ipconfig | KEYPLUG (Linux)

Chi

TOOLS

Trellix Insights

Trellix

Build a Strong Defence with Trellix

Hundreds of millions of ser
endpoint, email, web and r

One of the broadest and d
intelligence offerings on th

Critical context to prioritise
comprehensive cyber defe

ghts

LAS

e as a
TaaS)

Global Threat Intelligence (GTI)

Private GTI

Threat Intelligence Exchange (TIE)

Trellix

Trellix Threat Intelligence Group (TIG)

Resident Analyst:
- Full-time, dedicated analyst
- On-site, remote or hybrid
- Directed research

Intelligence as a Service:
- Team of remote analysts
- RFI-based research and analysis
- Advisory

Actionable intelligence and advanced analytics

Insights into developing threats, trends and vectors

Situational awareness of internal and external influences and threats

Trellix

Customer-Centric Offerings for Any Maturity

TACTICAL

LOW MATURITY

Least mature organisations with intelligence needs, with no teams or tools

GTI / TIE

Customer Need:
Out-of-box solution for in-depth threat detection, reporting and mitigation

TACTICAL / OPERATIONAL

MEDIUM MATURITY

Organisations with intelligence needs but no specialised team

INSIGHTS

Customer Need:
Proactive prevention of advanced attacks with complete life attack lifecycle protection

OPERATIONAL / STRATEGIC

HIGH MATURITY

Organisations with complete threat intelligence and hunting teams

ATLAS / PRIVATE GTI

Customer Need:
Global intelligence into APTs with key support for air-gapped environments

Customer Need:
White-glove, customised threat intelligence delivered as a service with a dedicated, expert and global threat intelligence team

INTELLIGENCE AS A SERVICE (INTAAS)

Trellix

Customer-Specific Intelligence Profiles

THREAT ACTOR PROFILE

Intelligence Team

Briefing for Executives and Managers

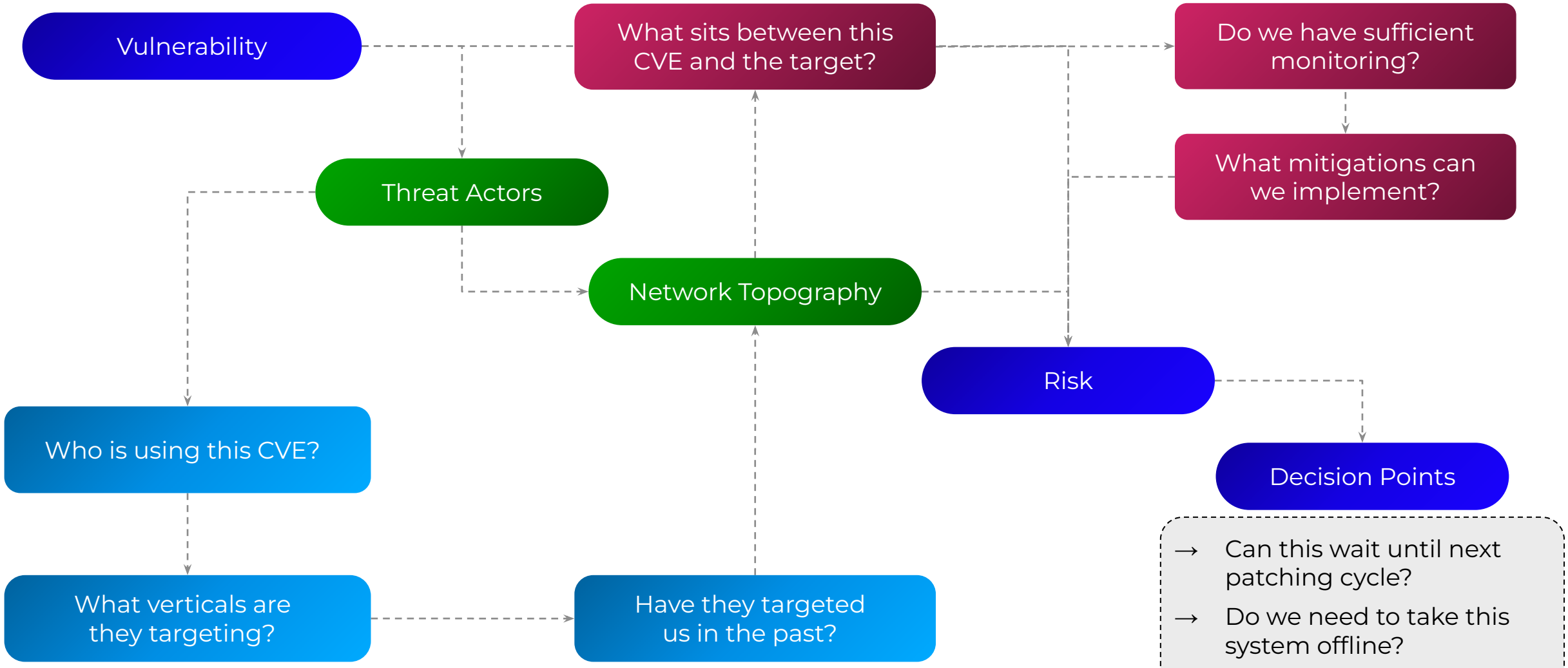
- Actor Motivations
- Organisational Risks
- TTPs
- Actor Capabilities

Technical and Incident Response Support

- Key Targets
- Hunt Rules
- Incident Response
- Compromise Assessment

Trellix

Digging Beyond The Surface



Trellix

Intelligence Support to CISO and Executive

WHY SHOULD THE COMPANY SPEND ON CYBER SECURITY?

Understanding **The Threat Landscape**

Understanding **The Business Mission**

Understanding **The Political Environment**

Understanding **Your Environment**

Intelligence Team

DATA + EVIDENCE-BASED CONCLUSIONS ON WHY MONEY SHOULD BE SPENT

Trellix

Operational Threat Intelligence Foundation

EUROPOL EC3 European Cybercrime Centre

CIRCL MISP Threat Sharing

JOINT CYBER DEFENSE COLLABORATIVE

NCA National Crime Agency

JPCERT CC

INTEL471

CYBERVEILIG NEDERLAND

MANDIANT

1.5 PB
of data (samples)

8.75 TB
data processed per day

2B
email samples per day

250M
malicious file detections per month

Real-time, reliable, information to:

1. Anticipate threats
2. Detect and block threats
3. Accelerate informed responses

Trellix

Trellix CyberThreat Report 2024

Trellix ADVANCED RESEARCH CENTER

THE
CYBERTHREAT REPORT

Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligence

- → GEOPOLITICAL EVENTS IMPACTING THE CYBER DOMAIN
- → RAPID AND SIGNIFICANT CHANGES IN THE APT LANDSCAPE
- → LOCKBIT SHAKES UP RANSOMWARE ECOSYSTEM
- → EDR KILLERS EMERGE
- → GENERATIVE AI AND THE CYBERCRIMINAL UNDERGROUND
- → U.S. PRESIDENTIAL ELECTION THEMED SCAMS

Trellix