Cisco Advanced Malware Protection

AMP everywhere and Cisco Visiblity

Agenda

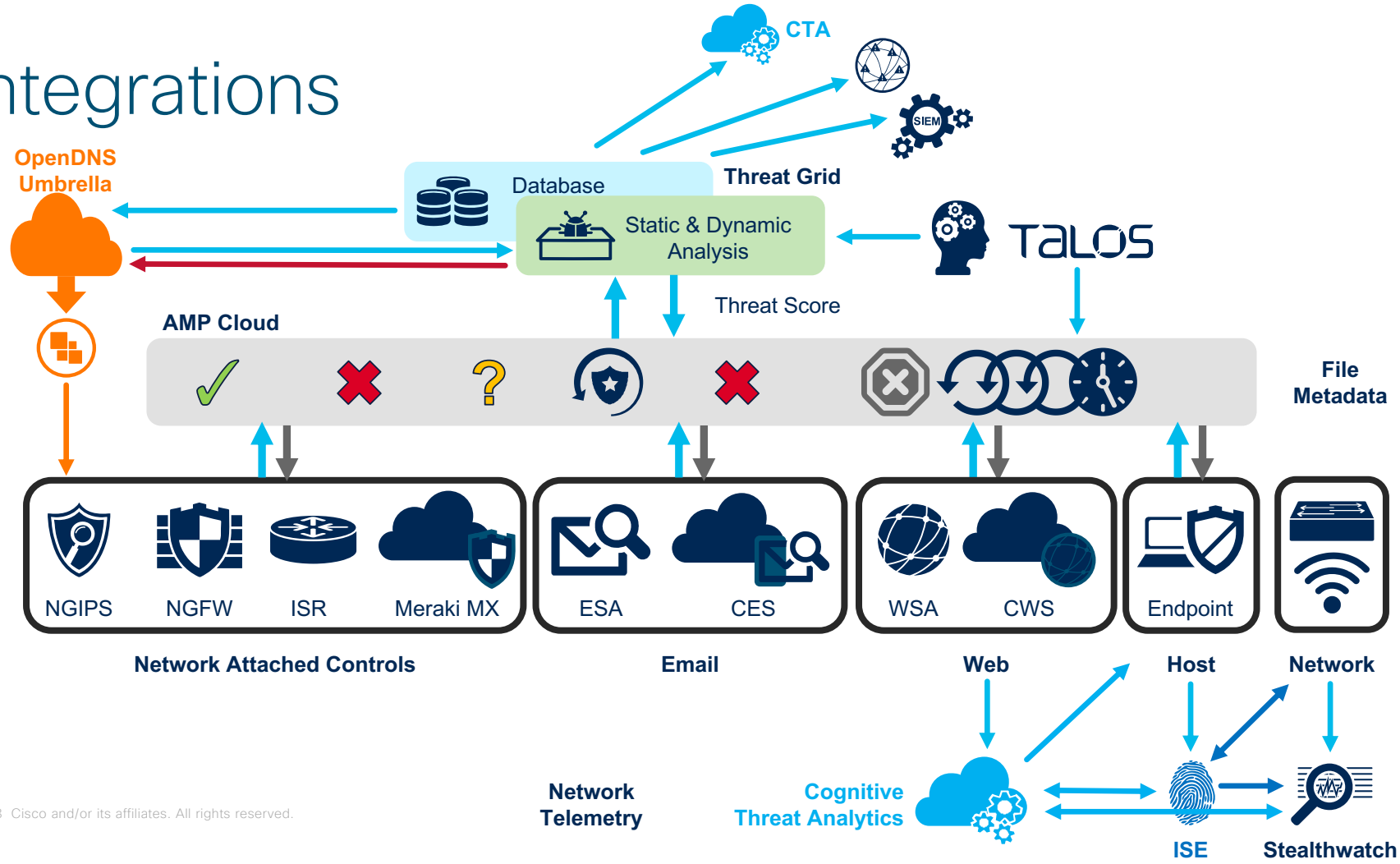
- AMP Architecture
- Events vs. Context
- How to generate Context
- Traditional Approach
- Context approach

The result of an analysis is generating information

Bringing this information into relationship is context

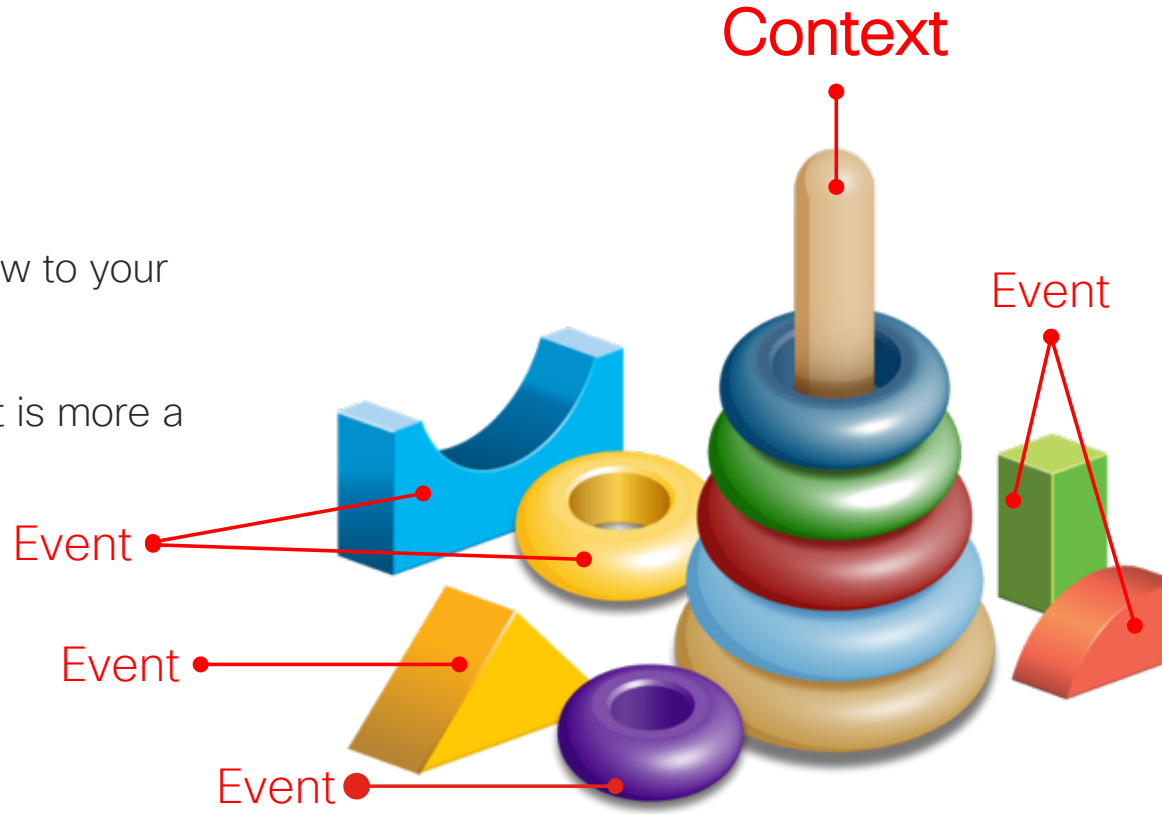
Context is needed to see the unknown

Integrations



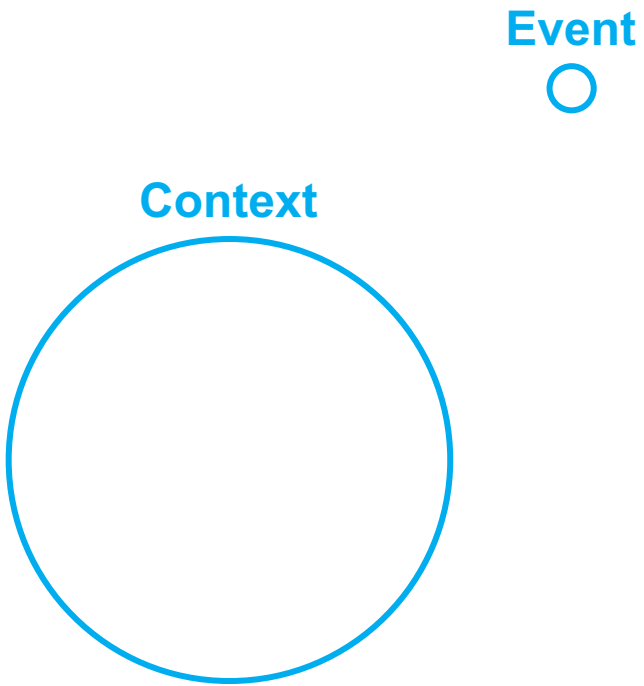
From Event to Context

- Context simplifies complexity
- Provides a complete different view to your insight threatlandscape
- Context aware is not a product, it is more a capability and approach
- Context is Relationship between Events



From Event to Context

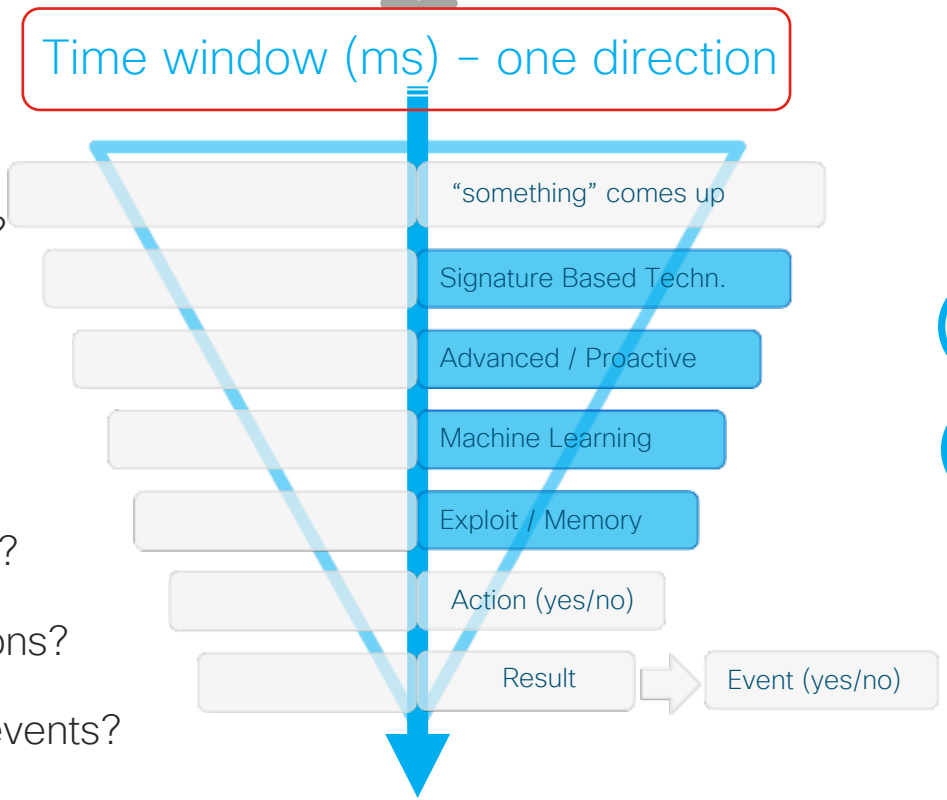
- Which point of view you need?
- Sophisticated „unknown“ in your environment is only available when looking at the context.
- Events are a small piece/part of information inside the context, but important.
- Knowledge what and how content must be correlated is the challenge
- Correlation without False-Positves is hard



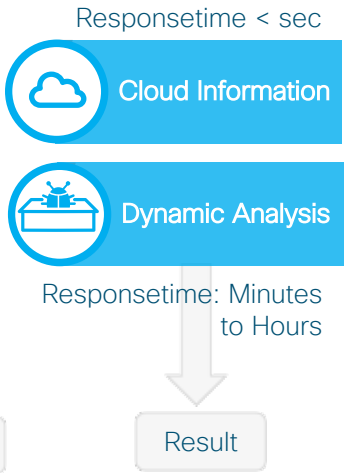
From Event to Context – Traditional Approach

Challenges

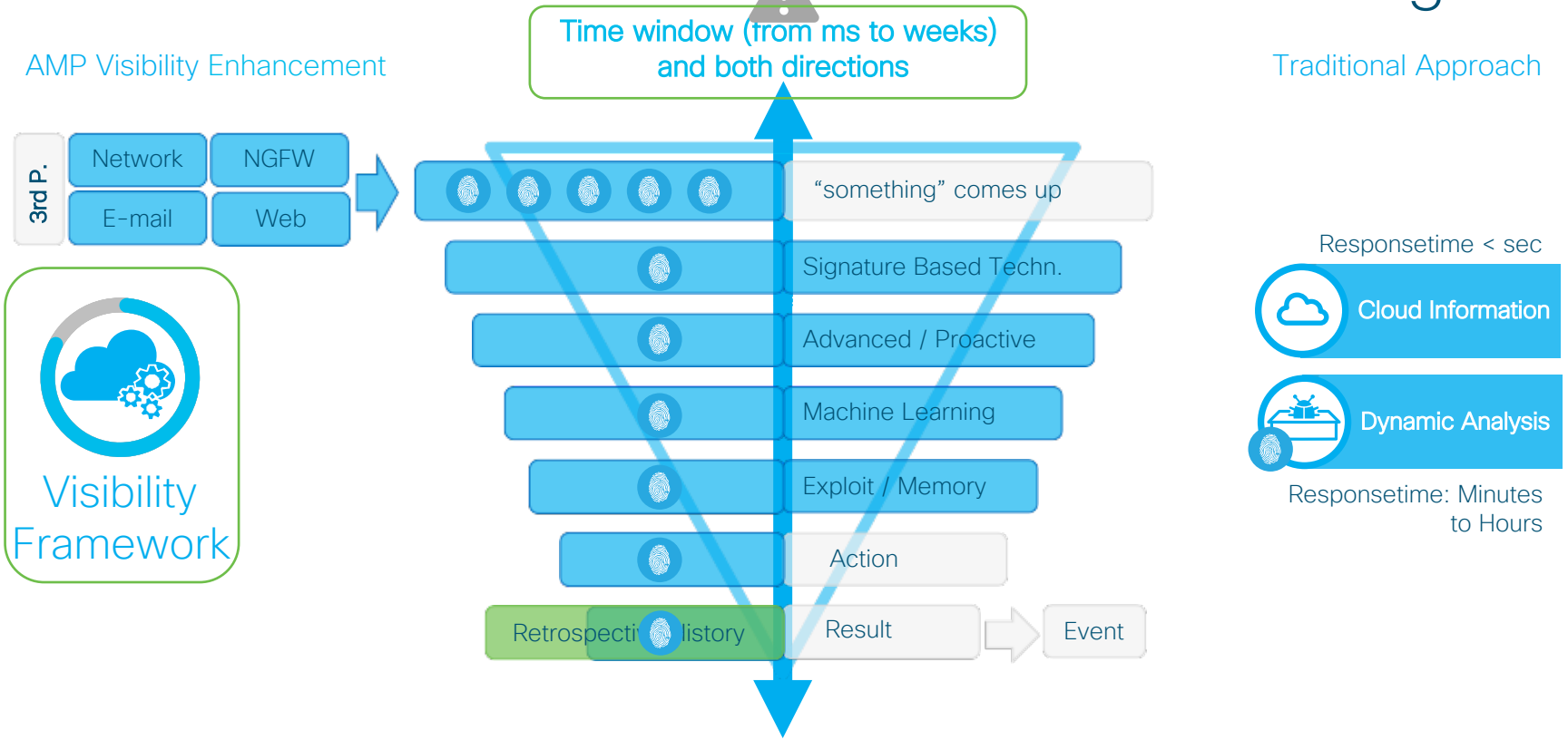
- All systems protected?
- Cloudservice available?
- When asking cloud?
- Dynamic Analysis – What / When
- Proper endpoint config?
- Monitoring normal actions?
- Monitoring non threat events?
- How Dynamic Analysis Results are handeled?



Traditional Approach



From Event to Context – Continous Monitoring



From Event to Context – Intelligence

Large Scale Datamining

Big Data Analytics and automated detection

Extensive Automation Framework

Understanding real world secenarios

Example with CTA

Anomaly Detection

Trust Modeling

Event Classification

Entity Modeling

Relationship Modeling

Services and Features not listed...

Cisco

Partners

3rd Party

Human Intelligence

Optional Services

IR Services

SOC Services

20B reqeusts to 20k incidents per day

From Event to Context – Retrospective

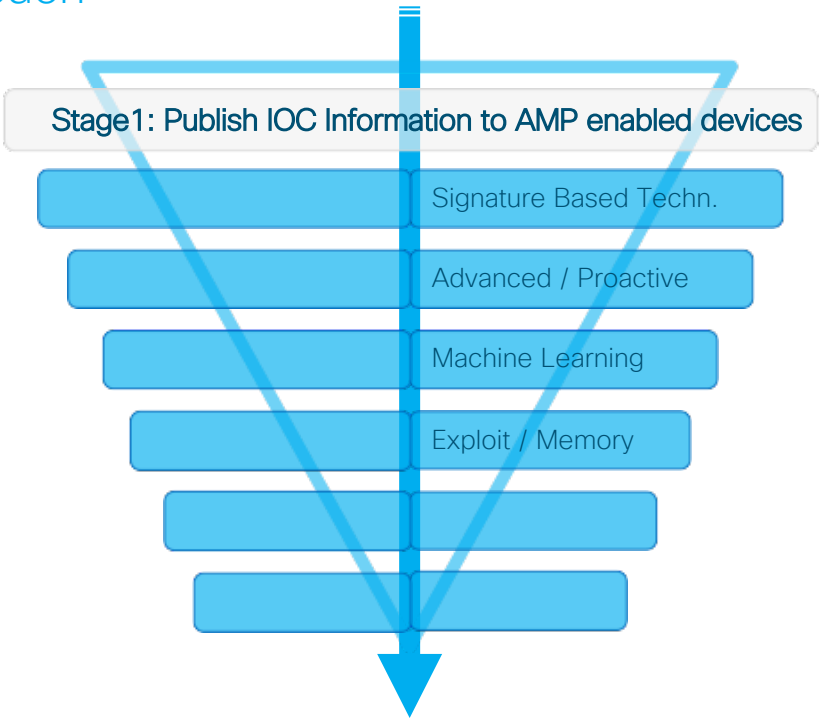
AMP Visibility Approach

3rd P.

Network | NGFW

E-mail | Web

Visibility



Traditional Approach

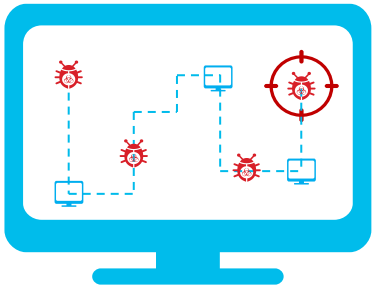
Cloud Information

Dynamic Analysis

From Event to Context – Retrospective

AMP Visibility Approach

Visibility



Stage1: Publish IOC Information to AMP enabled devices

Stage2: Look at the context

Identify a threat´s point of origin

See where it´s been?

See what it is doing?

Track it's rate of progression and how it spread

Examine target and remediate

Stage3: Answer Questions

What Happened?

Where did the malware come from?

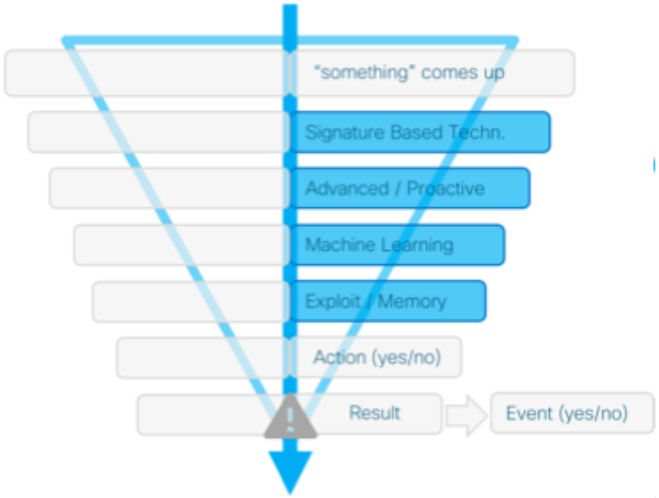
Where has the malware been?

What is it doing?

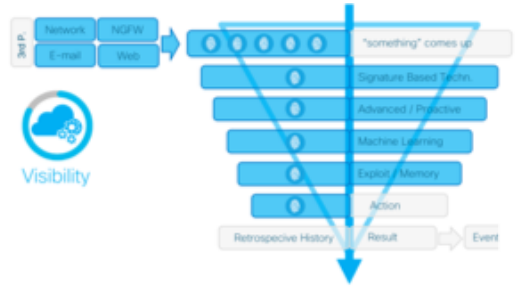
How do we stop it?

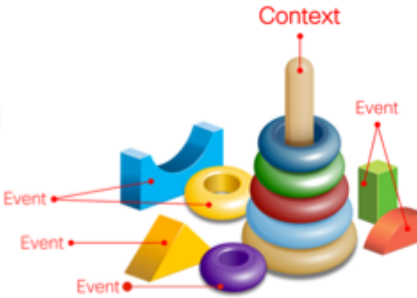
From Event to Context – Summary

Event Based
Traditional Approach



Context based
AMP Visibilty Approach



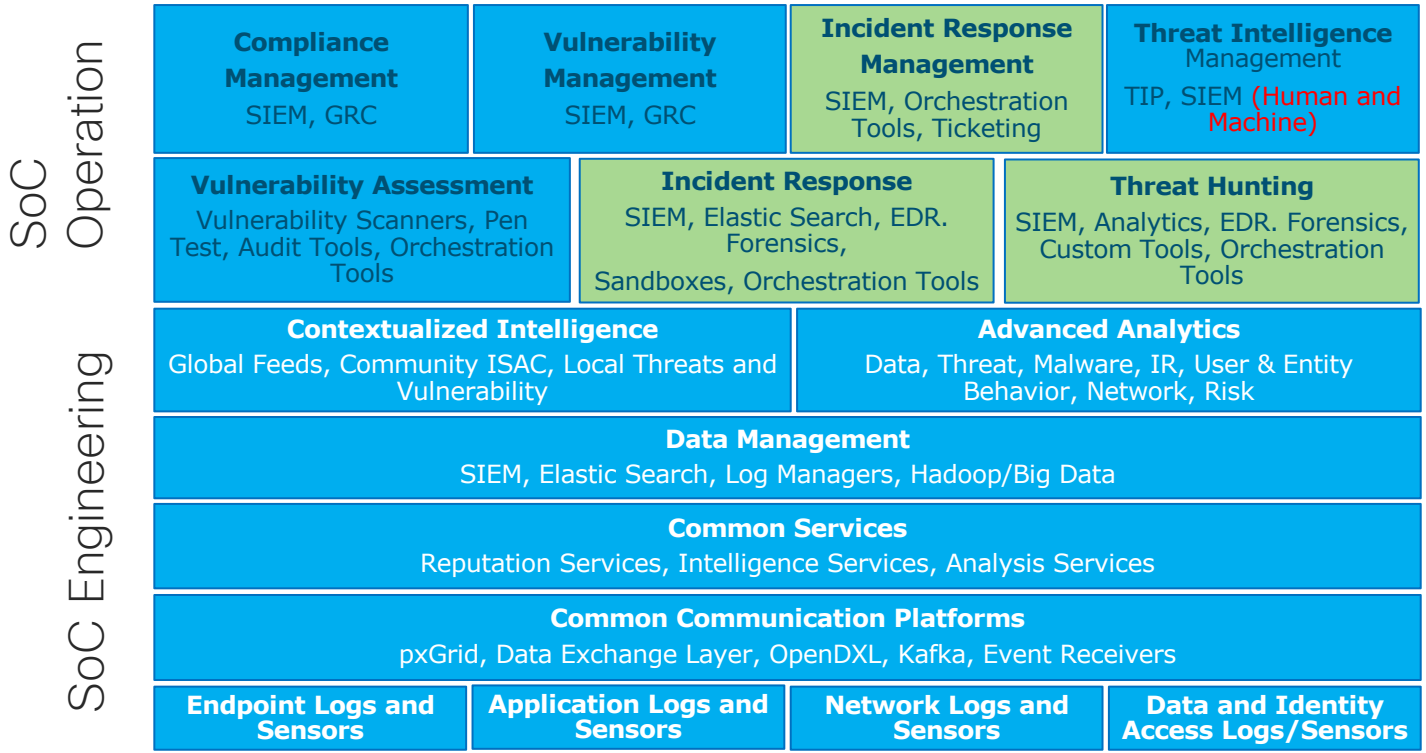


Q&A and Demo

Appendix 1

AMP Visibility from a Sec Ops Platform Architecture view.

Sec Ops Platform Reference Architecture View



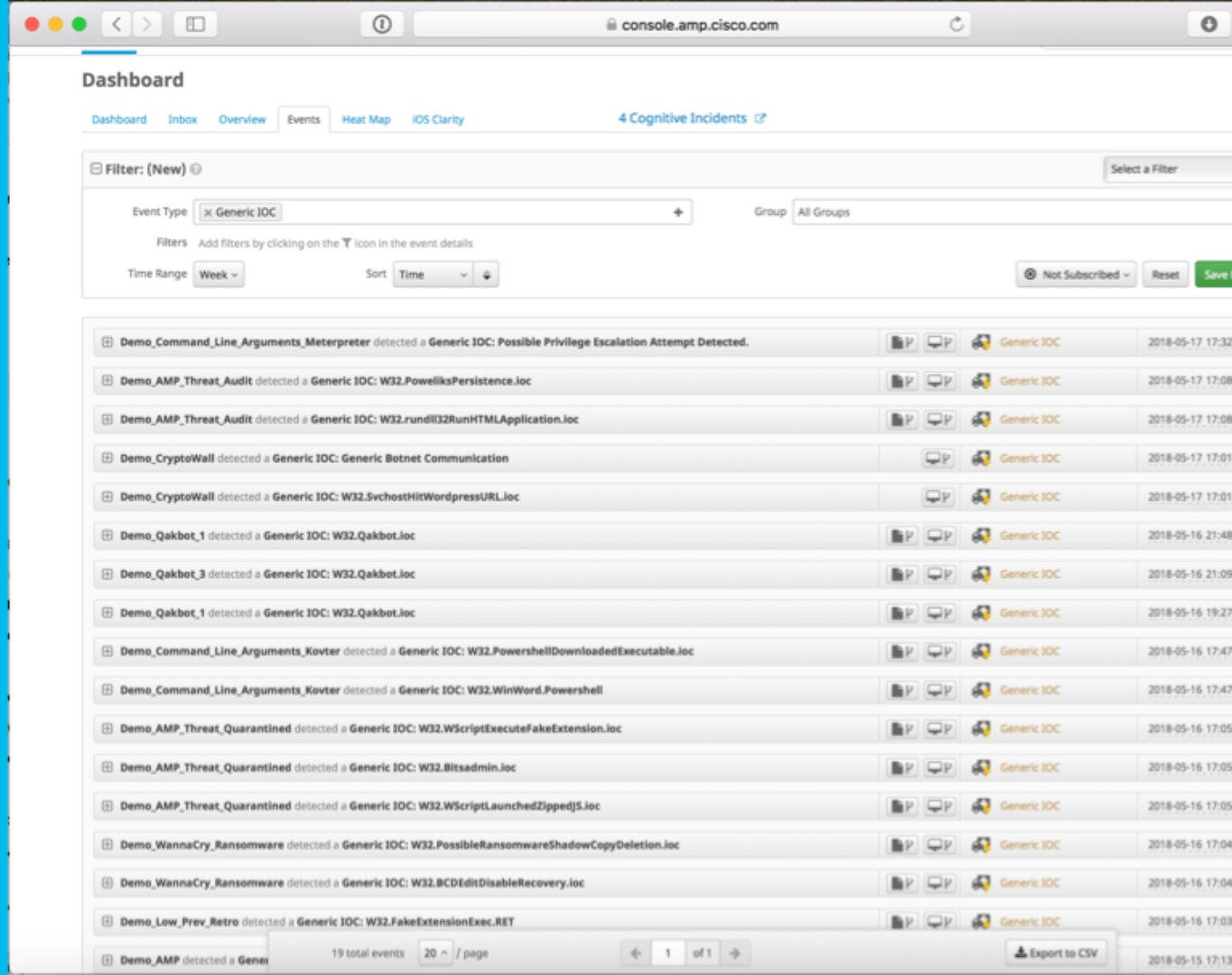
Appendix 2

Visibility Demo

I want to enrich all events and alerts so that I can detect, prioritize, correlate and respond to incidents by taking advantage of the capabilities of my infrastructure, effectively reducing the time to respond and remediate.

Sample IOC Events:

Event list for Generic IOC.

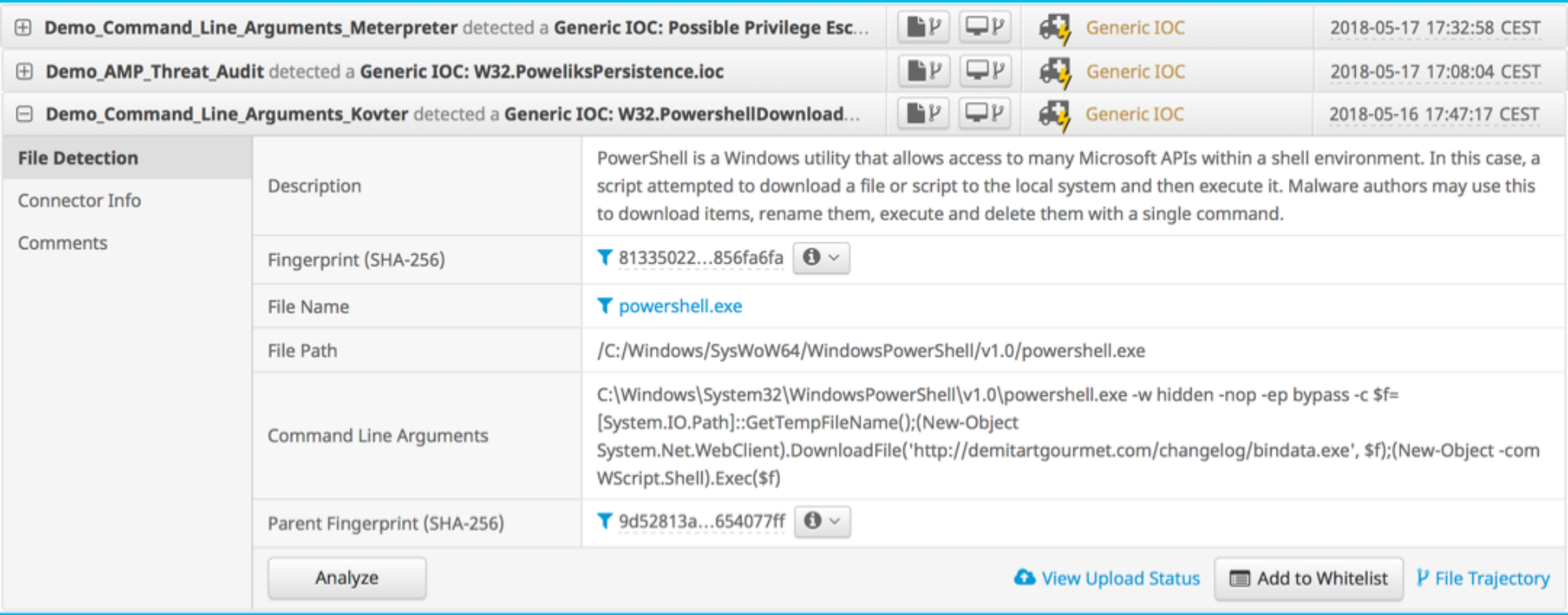


IOC Event Detail Examples

Generic IOC: W32.PoweliksPersistence

Generic IOC: Possible Privilege Escalation Attempt Detected

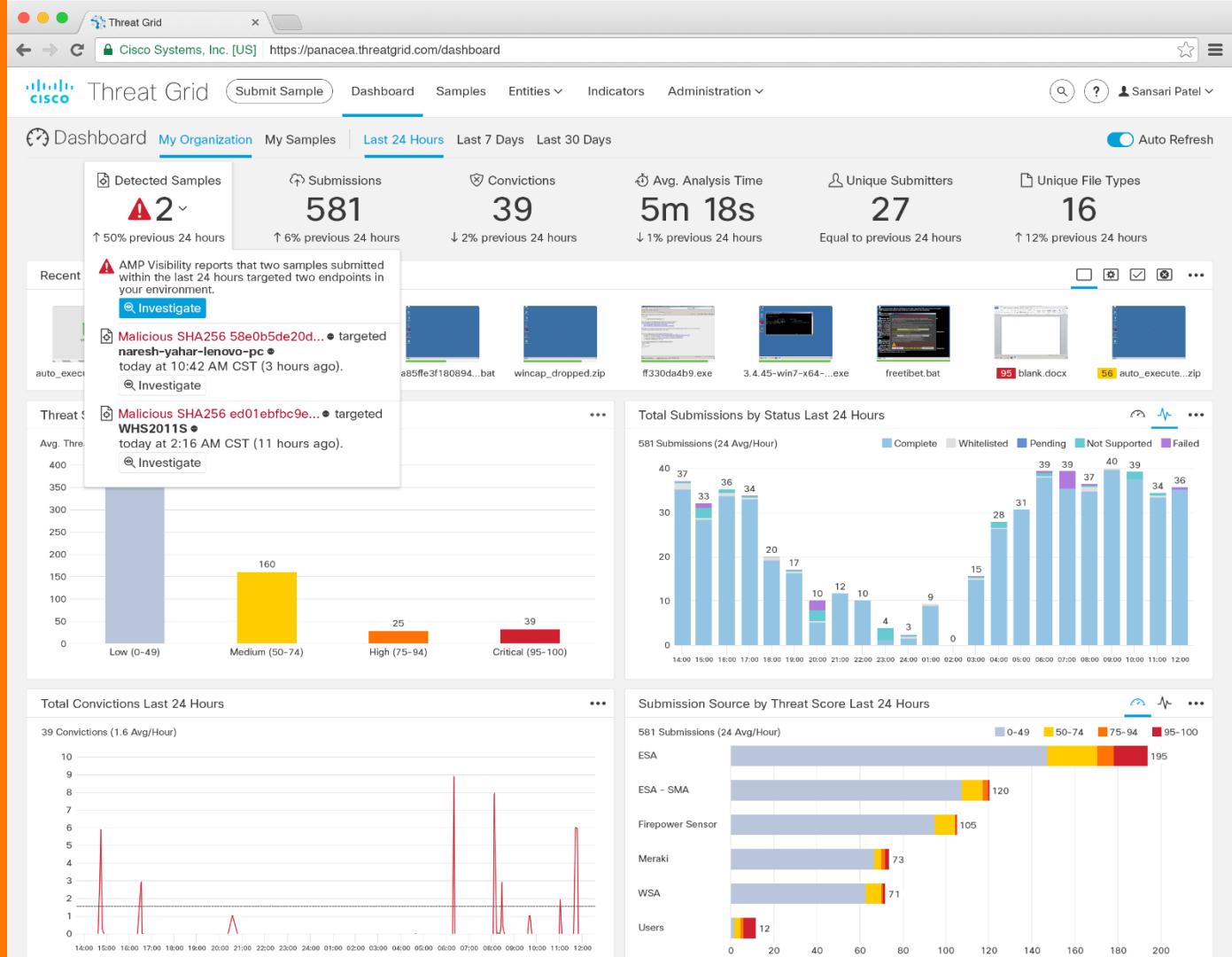
Generic IOC: Powershell Download



AMP Visibility Demo

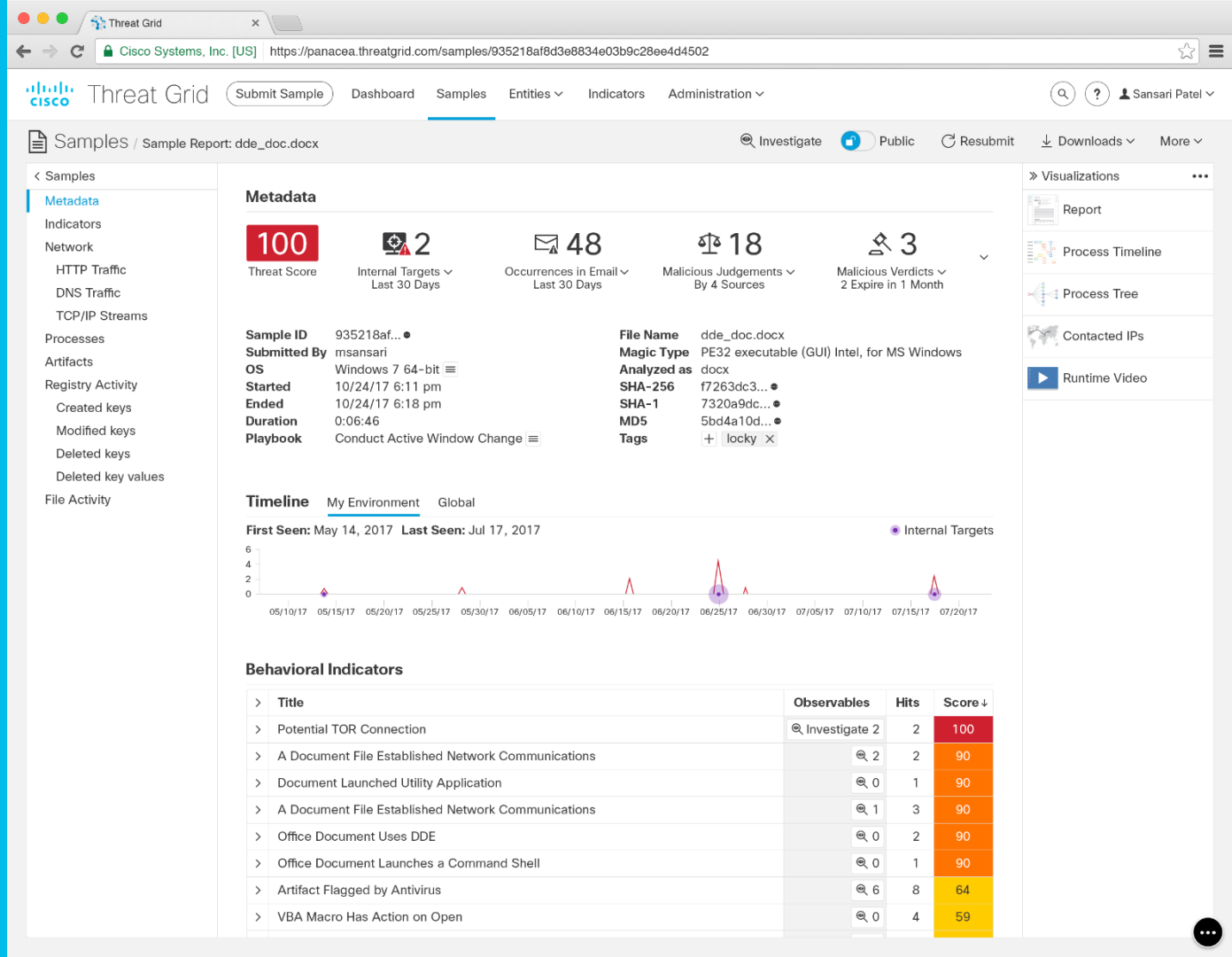
A Few New Items...

Dashboard: Integrated Data Sources



Sample Detail Page:

Sample report as user first view

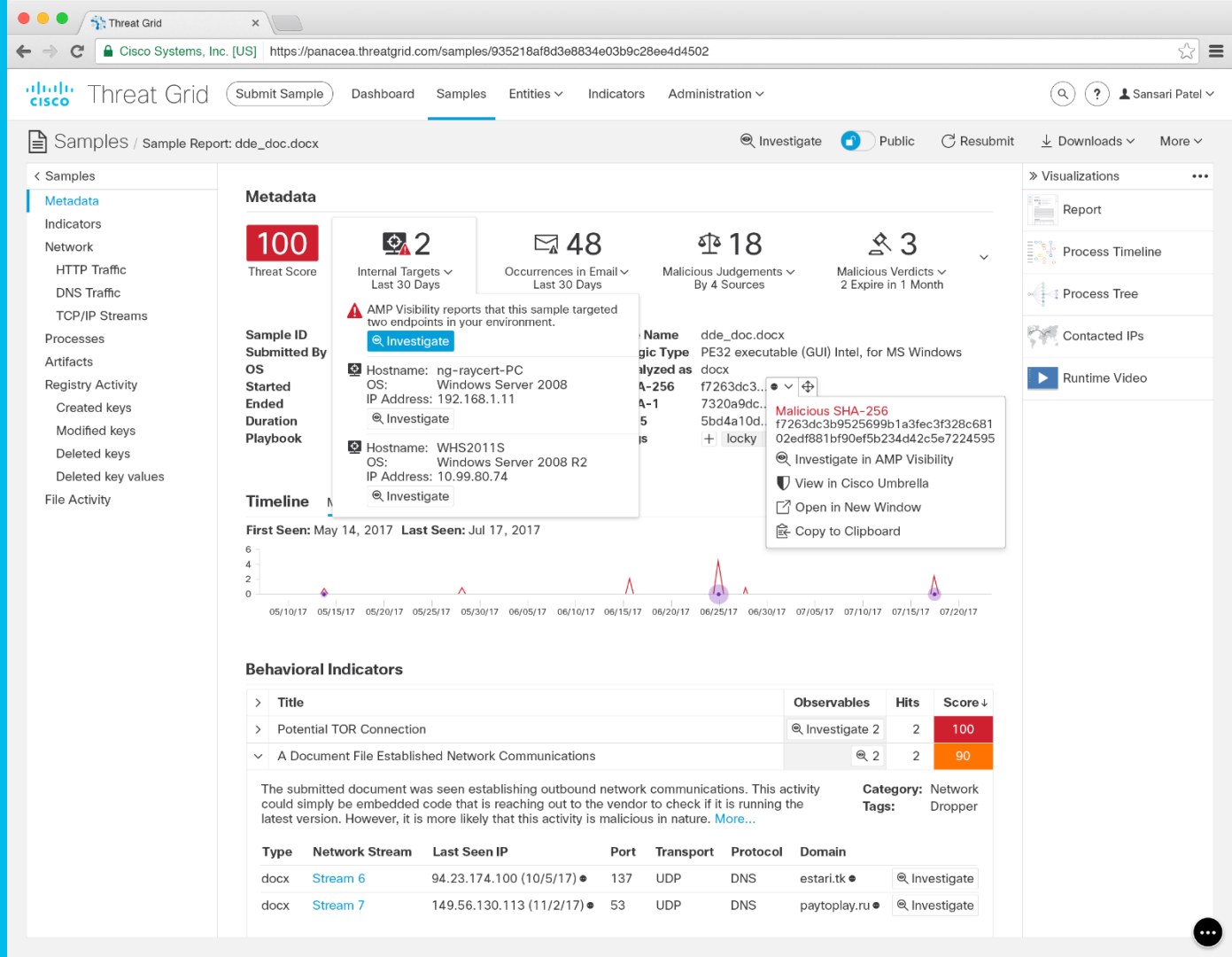


Sample Detail Page:

Internal targets menu expanded

Pivot menu expanded

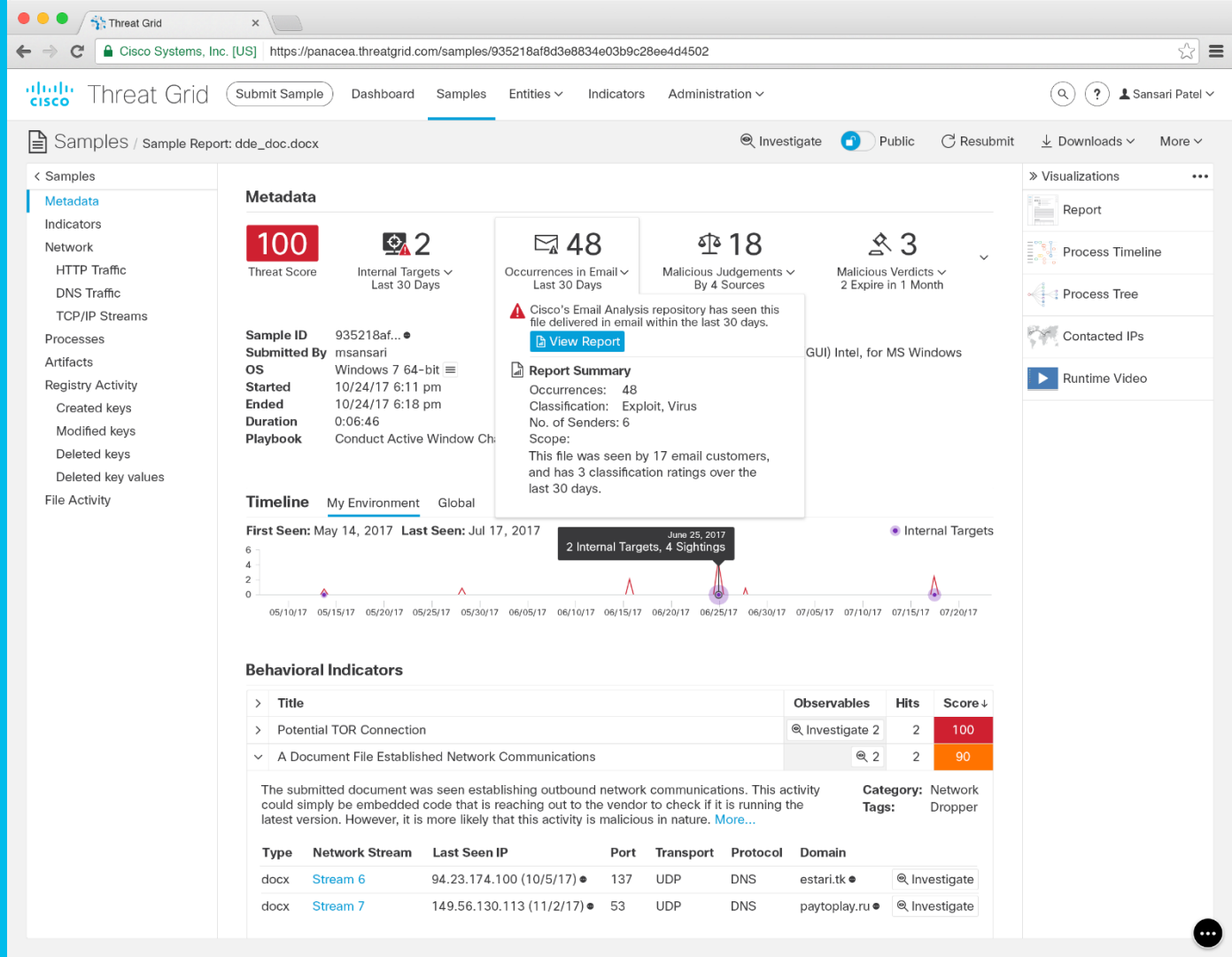
Indicators expanded



Sample Detail Page:

Shows Occurrences in Email Shows Timeline Target hover

Shows BI expanded

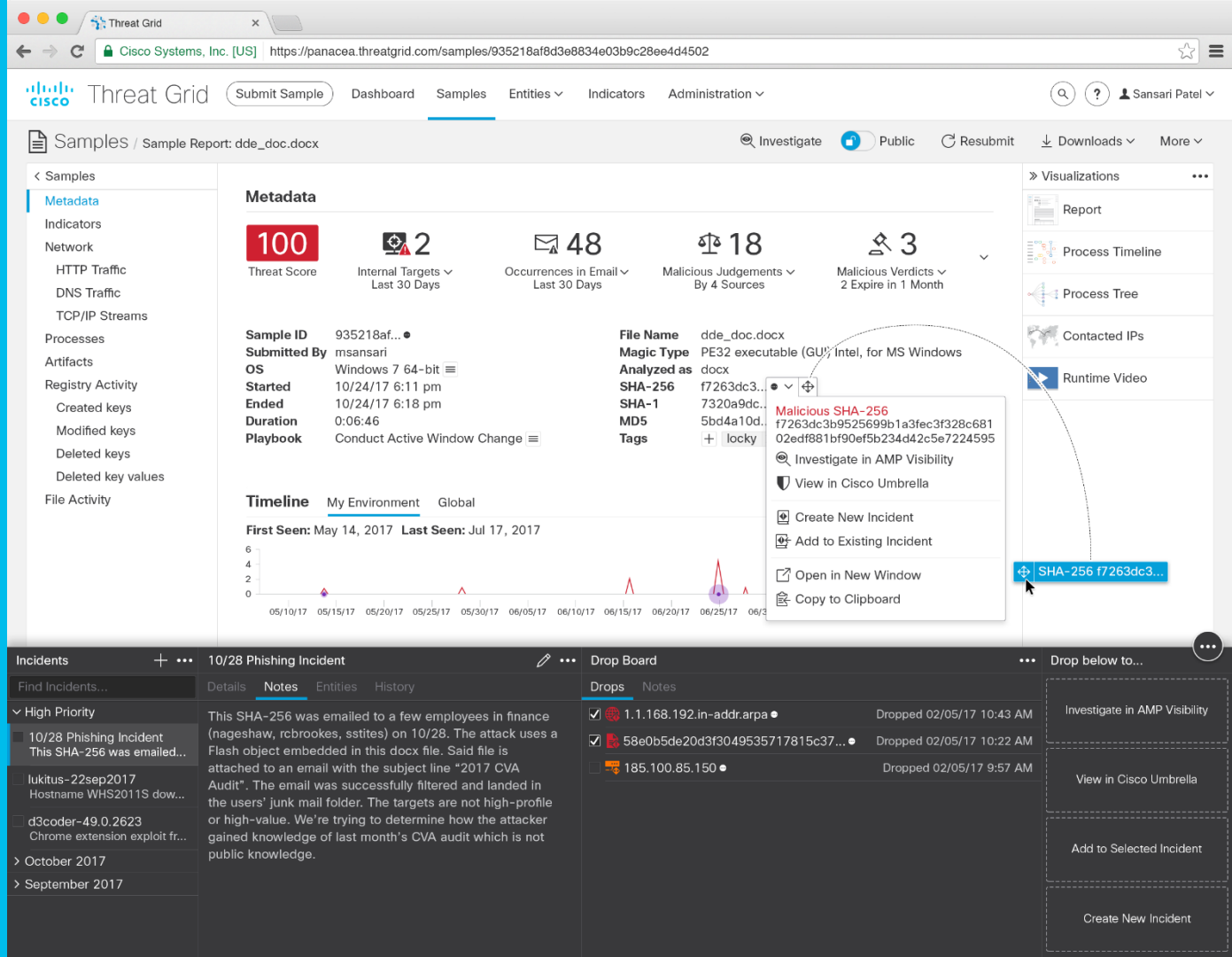


Sample Detail Page:

Incident/Drop Board expanded

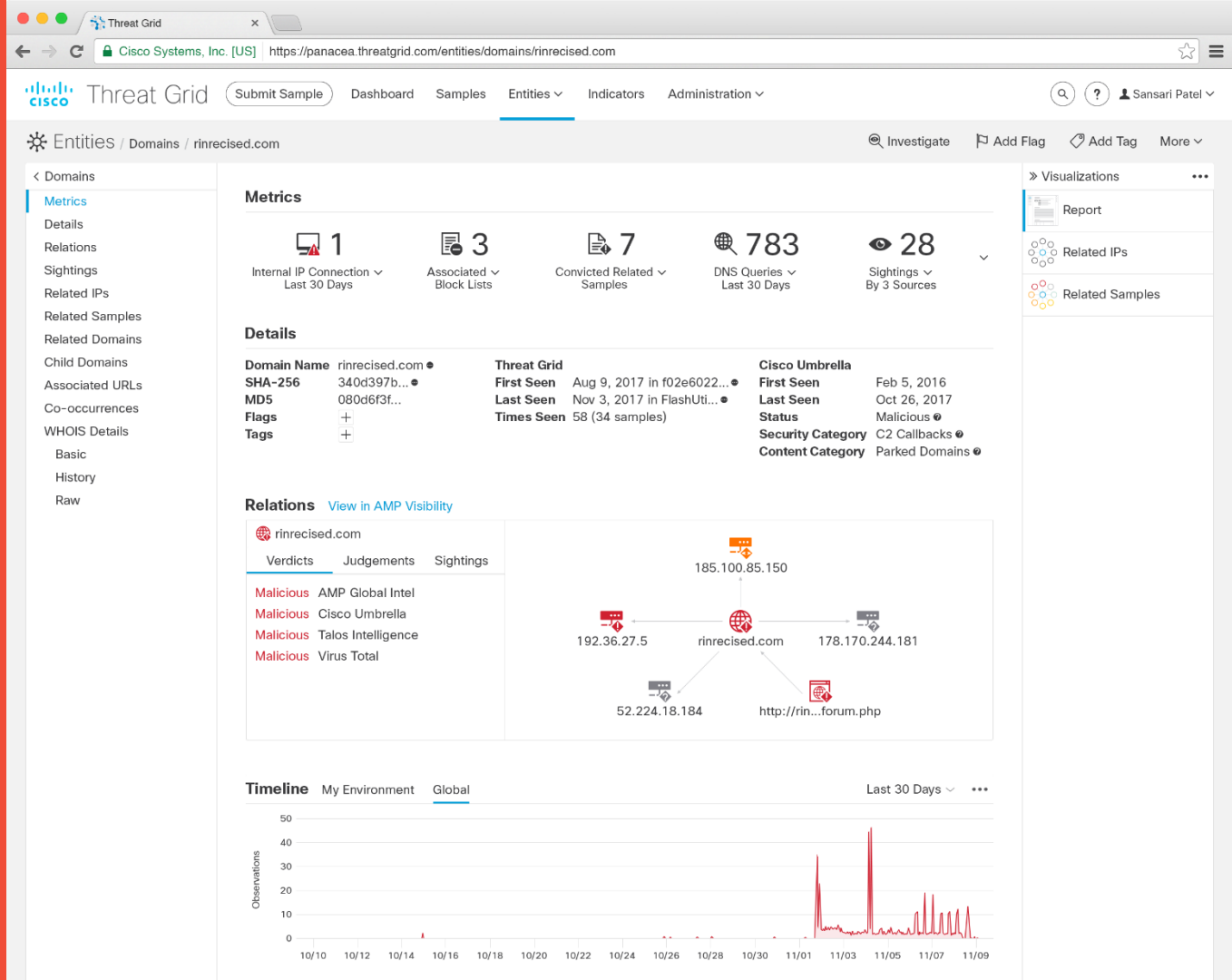
Pivot menu expanded

Drag & drop of entity



Domain Entity Page:

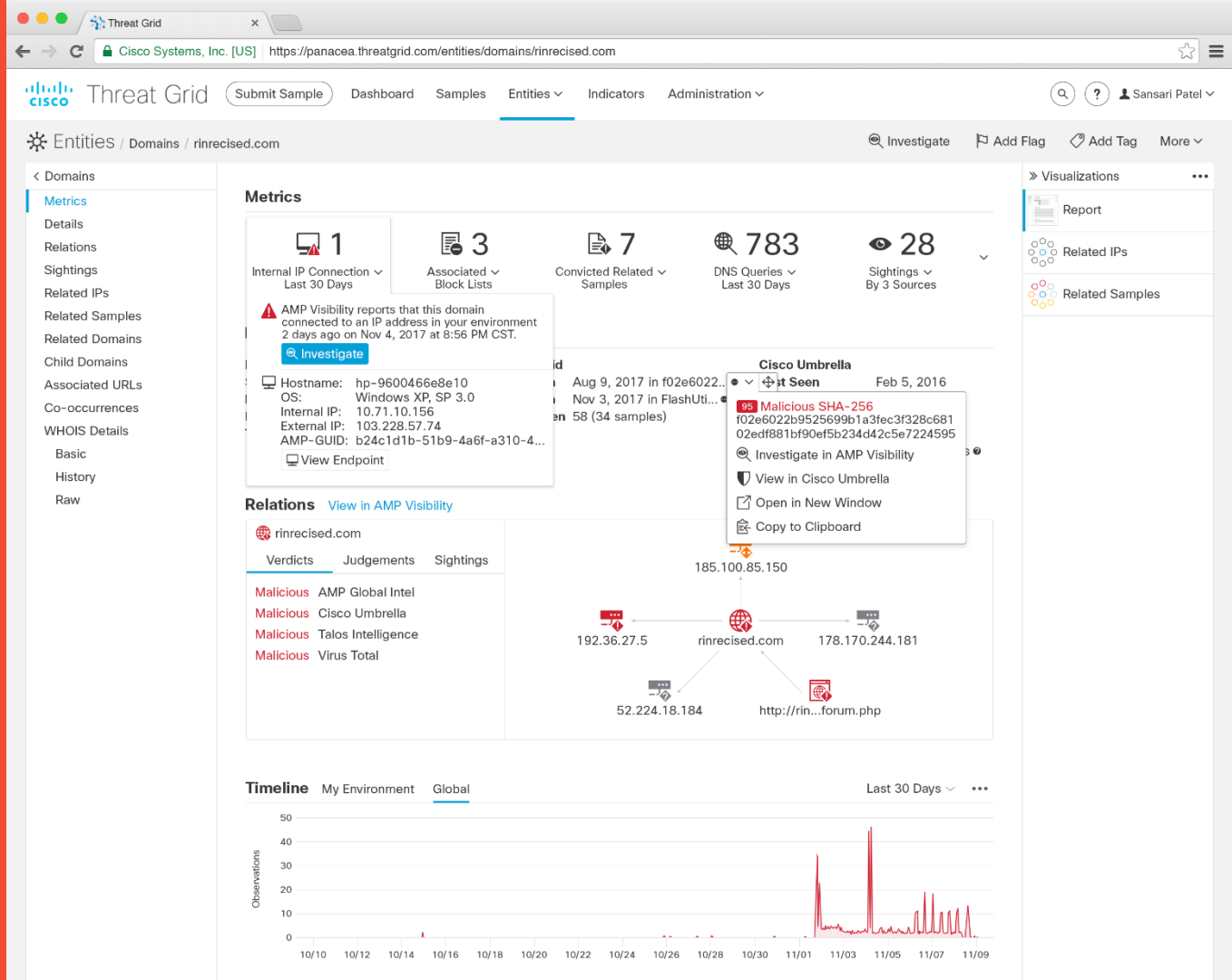
Domain page as user first views



Domain Entity Page:

Internal IP Connection menu

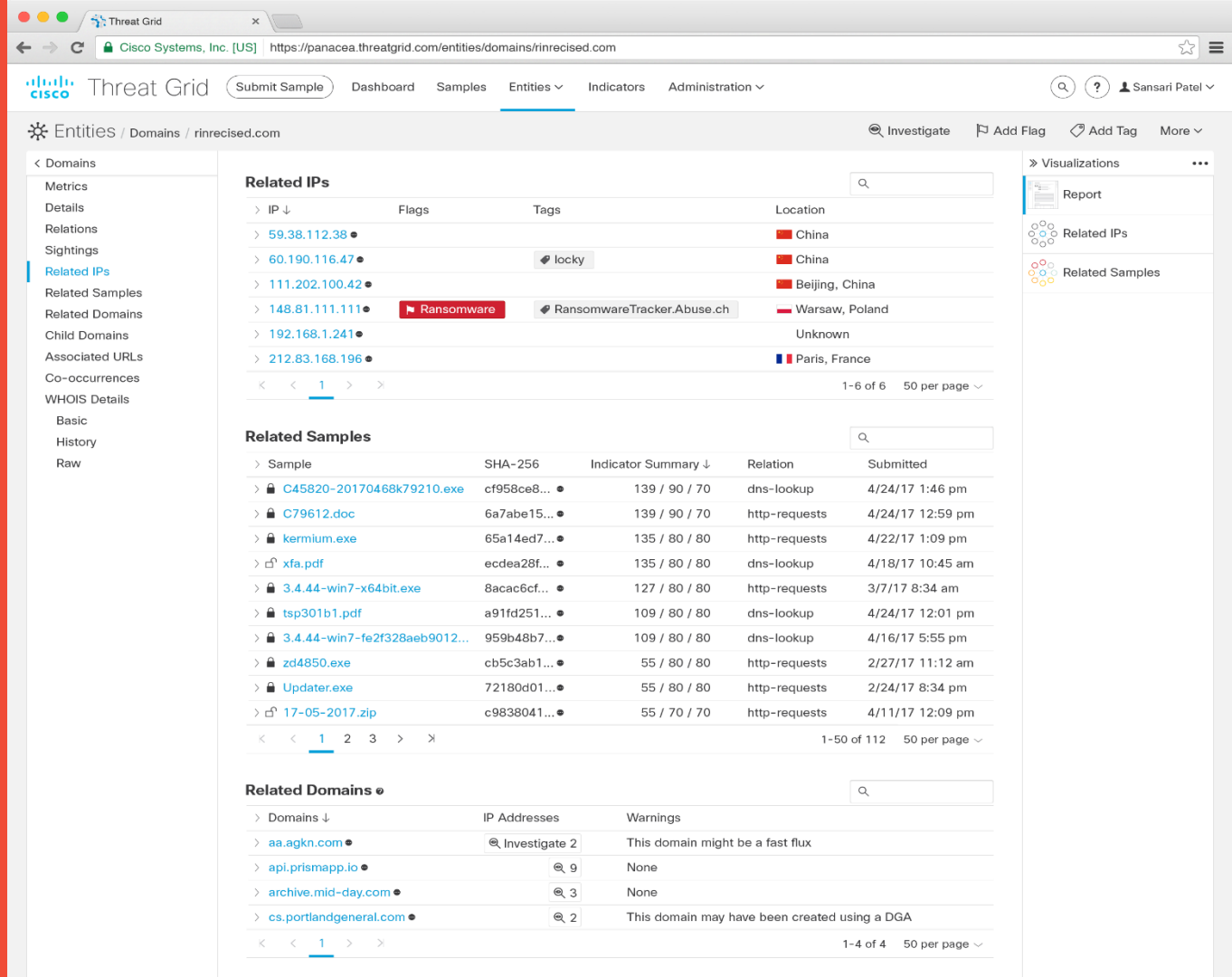
Pivot menu expanded



Domain Entity Page:

Related Entities

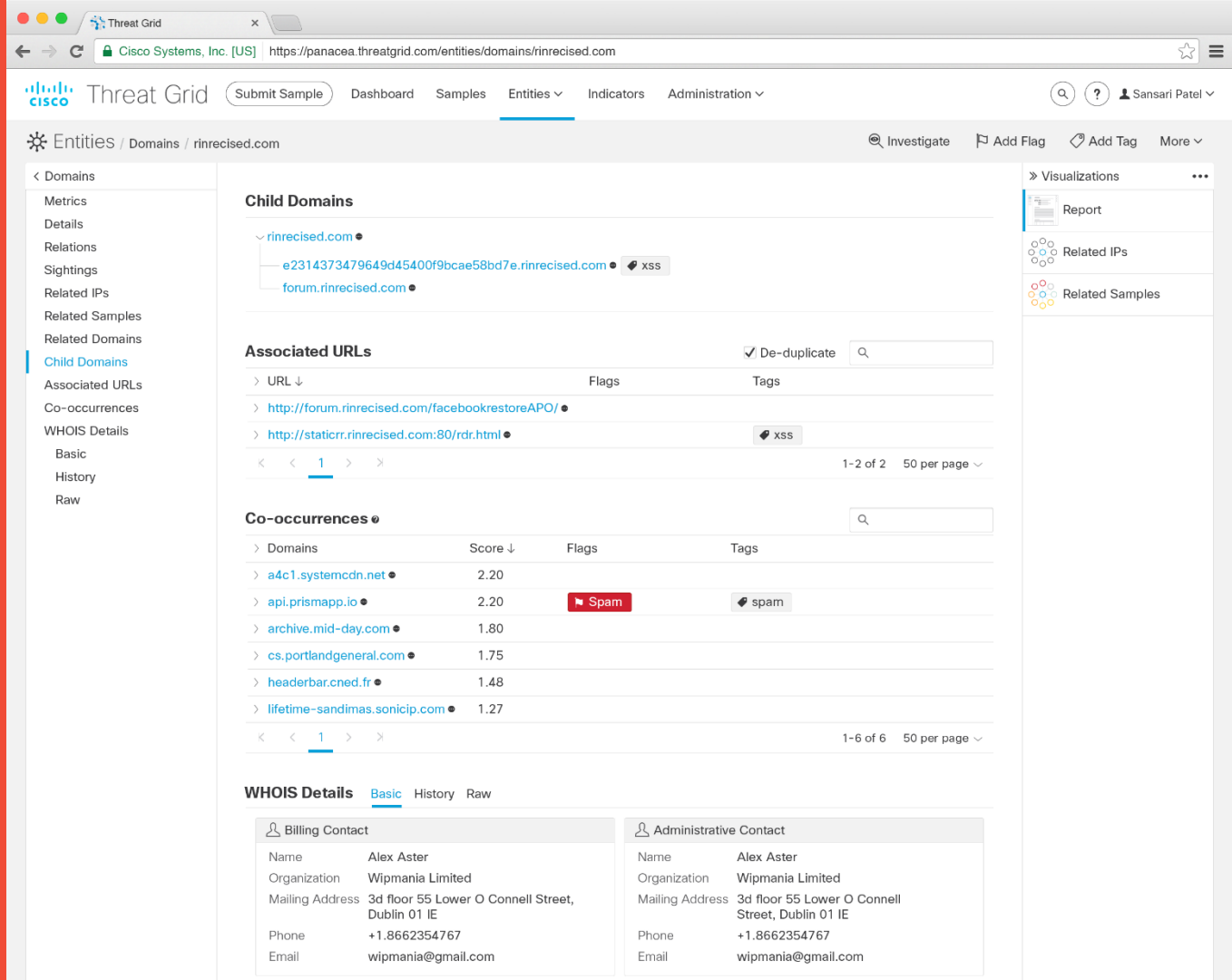
- IP Addresses
- Domains
- Samples



Domain Entity Page:

Related Entities

Cont.



Dashboard:

Detected Samples