About OmniSOC

- Shared 24/7/365-capable cybersecurity operations center for research & higher education (R&E).
- Led by/located at/leverages IU: Data Centers, GlobalNOC, InfoSec team, HR, legal, office space, etc.
- Average volume across all members: > 16 TB/day; > 17.2 B events/day; > 200k EPS.
- Elastic is key technology partner.

OmniSOC: always watching:

- **OmniSOC Core Service:**
  - 24/7/365 monitoring and alerting
  - SIEM (dashboard) access
  - Project Liaison:
    Onboarding support, single POC for emerging issues, interpretation, coordination of mass security events.
- SOC - Plus:
  - Honeypots, SIEM build/replacement, EDR, managed vulnerability scanning
- Cybersecurity Staffing Services:
  - Embedded, fractional- FTE: CISO, CISO advisory,, partial FTE security analysts/engineers, virtual cybersecurity teams, specialized IR teams, SOC readiness assessment, research- specific cybersecurity consulting.

Key features

- 24/7 network monitoring/threat hunting capability @ lower cost than hiring on-premise staff.
- Provides only actionable alerts.
- Community “herd immunity:” Leverages threat intelligence gained from across all members’ data.
- Cybersecurity staffing services (partial-FTE staffing)
- Higher Ed collaborator/ higher Ed focus.
- Helps meet insurance SOC requirements.
- Leverages MITRE ATT&CK framework.
- Acts as extension of member’s local security team.

OmniSOC

Current Member Community

Regional Networks

- I-Light/Indiana GigaPOP
- Connecticut Education Network (CEN)
- Southern Crossroads (SoX)

NSF Facilities

- Academic Research Fleet
- NOIRLab
- National Radio Astronomy Observatory
- ACCESS

Higher Education

- University of California Santa Cruz
- Case Western Reserve University
- Claremont Colleges*
- Clemson University
- University of Connecticut
- Creighton University
- DeSales University
- Fordham University
- Indiana University
- Lehigh University
- Lehigh Carbon Community College
- University of Nebraska
- Northwestern University
- Purdue University
- Rutgers University
- San Diego State University
- Santa Clara University
- Stony Brook University
- Virginia Tech
- University of Wisconsin System

*Finalizing contract

OmniSOC

Why not DIY?

- $67k ELK server, storage cluster, and software licensing to build monitoring system
- $95,380k/year (average salary, Glassdoor) security engineer salary, x 1.5 for tax and benefits, x 4 for 24/7/365 coverage = $572,280
- $50k/year to provide professional development and training to keep this staff up to date on the latest techniques and technologies

~$689,280 year 1

~$600,000 each year following

How OmniSOC Works

Log Requirements

Must Have (Required)

- **Traffic Session — N/S**
  - e.g. Netflow, Zeek, Conn logs
- **NIDS**
  - e.g. Suricata, Palo Alto Threat logs
- **DNS query logs**
  - e.g. Bind, Zeek DNS
- **Endpoint logs for critical systems**
  - e.g. Crowdstrike, Elastic Endpoint, MS Defender

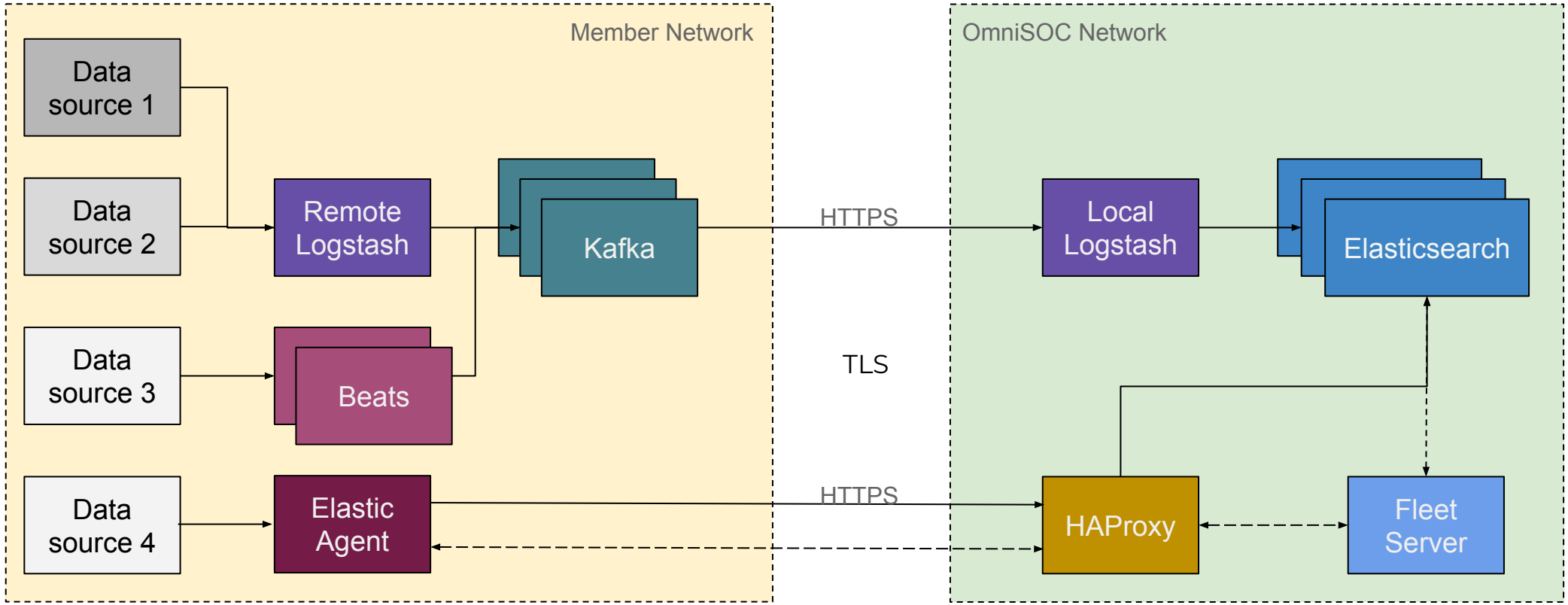
Adds Significant Value

- **Application layer protocol analyzers**
  - e.g. Zeek, HTTP, SMTP, TLS, Weird
- **Centralized Authentication**
  - e.g. AD, kerberos, O365
- **Malware**
  - e.g. MS Defender
- **Web Proxy**
  - e.g. Palo Alto, Squid

Helpful—Not Required

- **NAT logs for public/private IP mapping**
- **DHCP**
  - e.g. Zeek DHCP
- **Traffic Session E/W**
  - e.g. Netflow, Zeek Conn logs
- **Endpoint logs for high value** (less than critical) **systems**
- **Wireless/VPN Authentication**
- **Vulnerability scanner results**
  - e.g. OpenVAS, Nessus, Qualys
- **Honeypots**
  - e.g. Duke STINGAR
- **Service-specific access logs**
  - e.g. MSSQL, MySQL, Apache

Typical Architecture



- ➔ Raw data collected by Logstash on aggregators
- ➔ Inserted into Kafka as-is
- ➔ Picked up by IU-based Logstash instances
  - ◆ “Store and forward”, no data loss due to network interruption

- ➔ Data normalized to ensure consistency between different sources
- ➔ Data augmented with additional metadata
- ➔ Finally indexed into Elasticsearch

OmniSOC

Daily incident and threat hunting

- Automated Detections
- NIDS Alerts
  - Newly encountered alerts
  - Recent alert spikes
- Known Bad
  - Previously actioned IoCs (Across all OmniSOC members)
  - External Threat Intelligence
- Ignore Known Good/False Positives
  - Know thy environment

Deeper hunting

- Manual Hypothesis Based Hunts
- Long Tail Analysis:
  - Unique metadata groups (e.g. Browser User Agents)
  - Least occurrence events
- Anomaly Detection
  - C2 Beaconing
  - Baseline Deviations / Machine Learning

Communications/Member operations

OmniSOC engages with members through:

- Tickets
- Email lists
  - Monthly Hunt Summaries
  - $NEWSINT Events
- Video Conferencing (Zoom)
  - Bi-Weekly Meetings: Platform Updates / Reported Incident Reviews
- Slack
  - Interactive discussions/ Information Sharing
- Hunt Journals/Case Management
- PL/VCS Engagement


OmniSOC
omnisoc.iu.edu

Becoming a member

Typical Use Case

Requirements	Typical Services	Funding Requirements
• **Higher education or research institution** • **REN-ISAC member**	• **Core Services @ 50-200 GB Level**	• **~$81K-$98K** ○ Managed 24x7 monitoring, alerting, actionable alerts, deep threat hunting

• **Defined resource to address alerts**
  ○ May be OmniSOC virtual staff
• **Has necessary logs**
  ○ Or funded plan to add
• **Funding for member fee**
	• **.25-.5 FTE virtual Cybersecurity staff**
	  ○ Onboarding lead + other tasks
		• **~$41K-$83K**
		  ○ 1 year, often extended to years 2, 3

	• **SIEM (dashboard) access**
	  ○ For security teams
		• **~$14K***
		  ○ Included in above Core Service figures

Onboarding: usually 12-14 weeks, begins & payment starts not earlier than 60 days after contract executed.

OmniSOC

Member Fees

Drivers

- Average log volume (GB/day)
- Data retention (30 days standard)
- Need for hosted SIEM
- Need for other services

For institutions with enrollments ~10,000-15,000 and ingest of 350-500 GB daily, OmniSOC can provide 24x7x365 monitoring & delivery of actionable alerts + deep threat hunting (Core Service) @ a cost less than 2 FTE.

OmniSOC

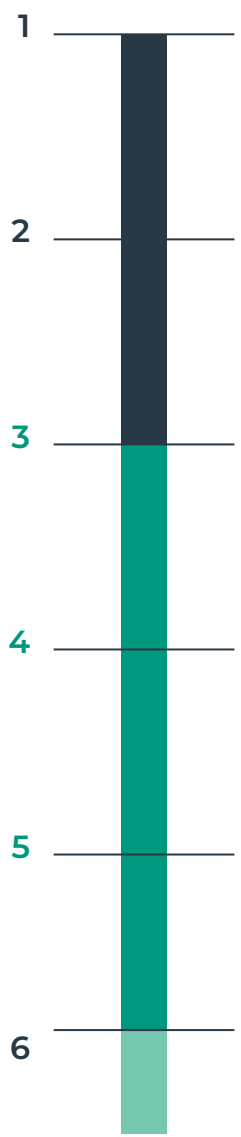
Member Fees

Drivers

- Average log volume (GB/day)
- Data retention (30 days standard)
- Need for hosted SIEM
- Need for other services

Historically, for institutions with enrollments ~ 5,000 and ingest of 50-150 GB daily, OmniSOC can provide 24x7x365 monitoring & delivery of actionable alerts (Core Service) @ less than the cost of one FTE/FTE with benefits.

Roadmap to membership



1 **Scoping and contracts**

Sizing, selecting right services, establishing contractual relationships,

2 **Deeper discovery**

Establish comms channels, better understanding of your infrastructure, create onboarding plan

3 **Onboarding: Platform**

Set up monitoring appliances and aggregators, assess feed quality, begin normalization and enrichment workflows, deploy endpoint solution

4 **Onboarding: Security Engineering**

Establish monitoring rules and workflows, begin threat hunting

5 **Onboarding: Virtual Services**

Get to know Project Liaison. Establish vulnerability scanning. Set up honeypot management platform. Intro VCS personnel.

6 **Move to production**

OmniSOC

OmniSOC

Thank you for your attention.

Questions?

omnisoc.iu.edu

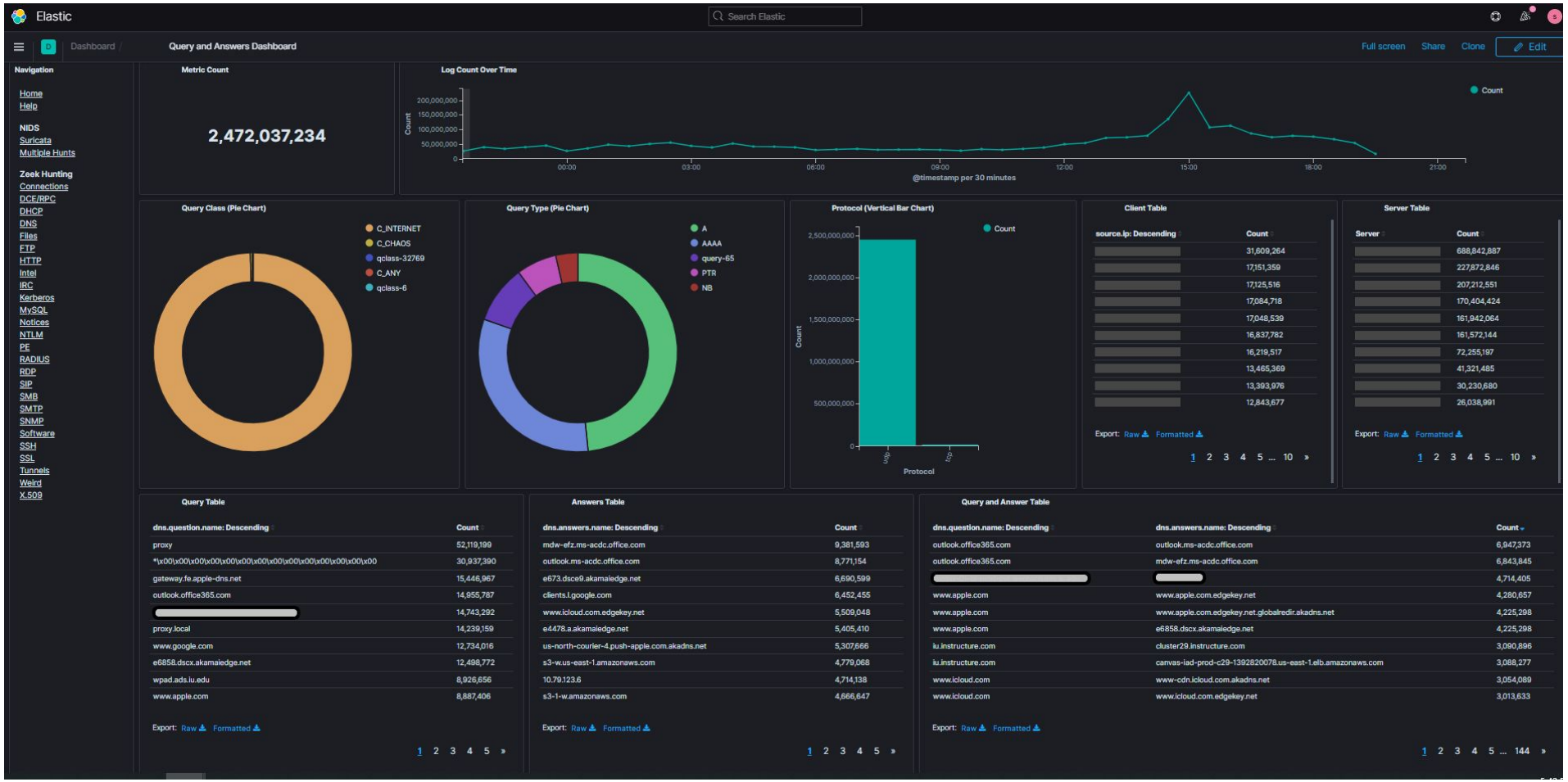
soc@omnisoc.iu.edu

toddston@iu.edu

Palo Alto traffic dashboard

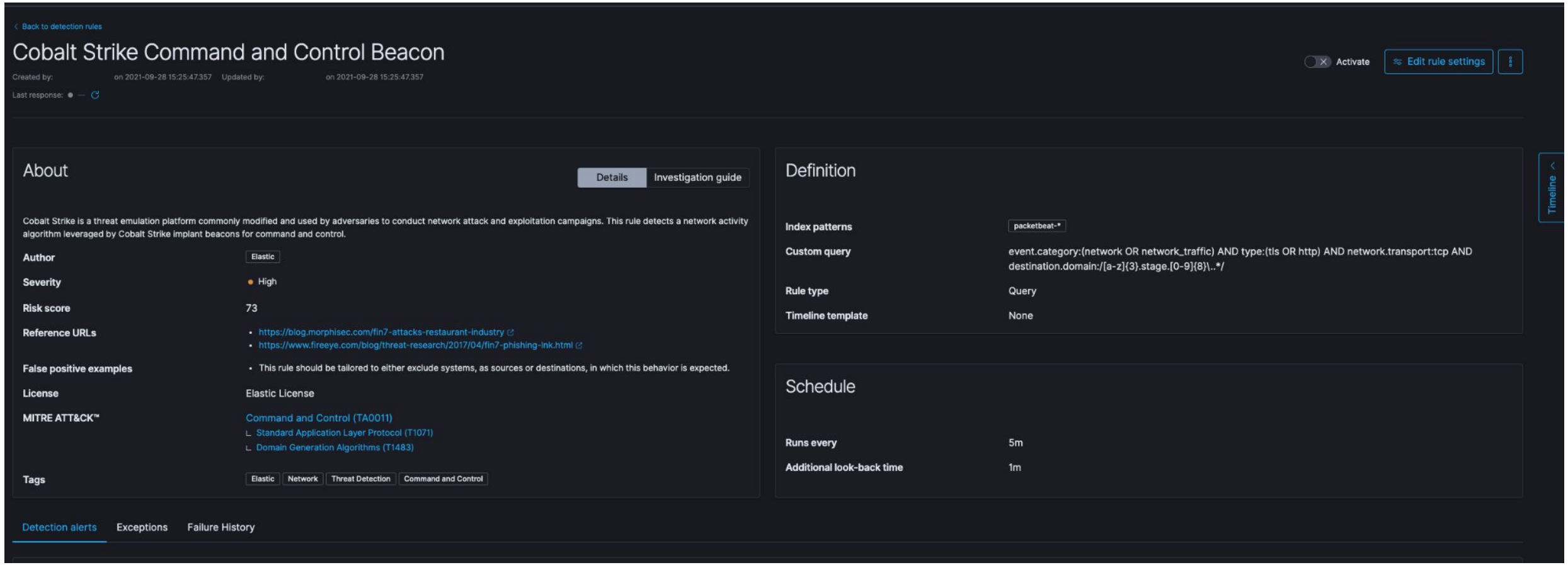
OmniSOC

Zeek DNS dashboard

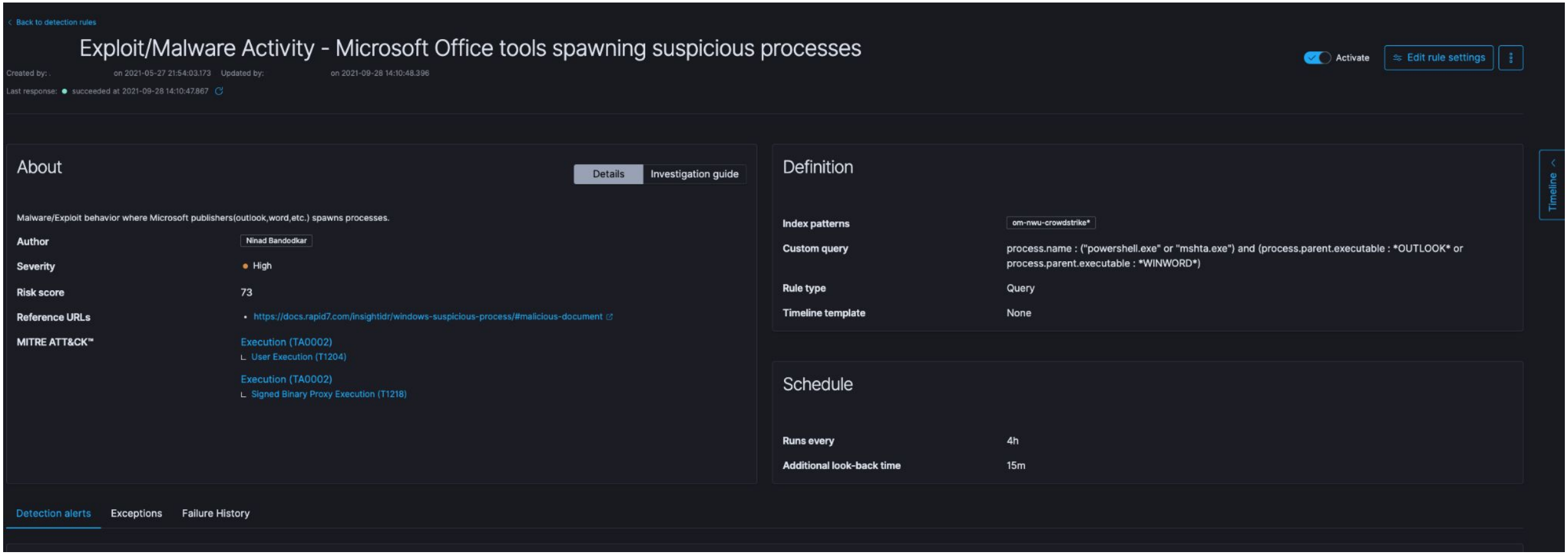


OmniSOC

Cobalt strike automated detection

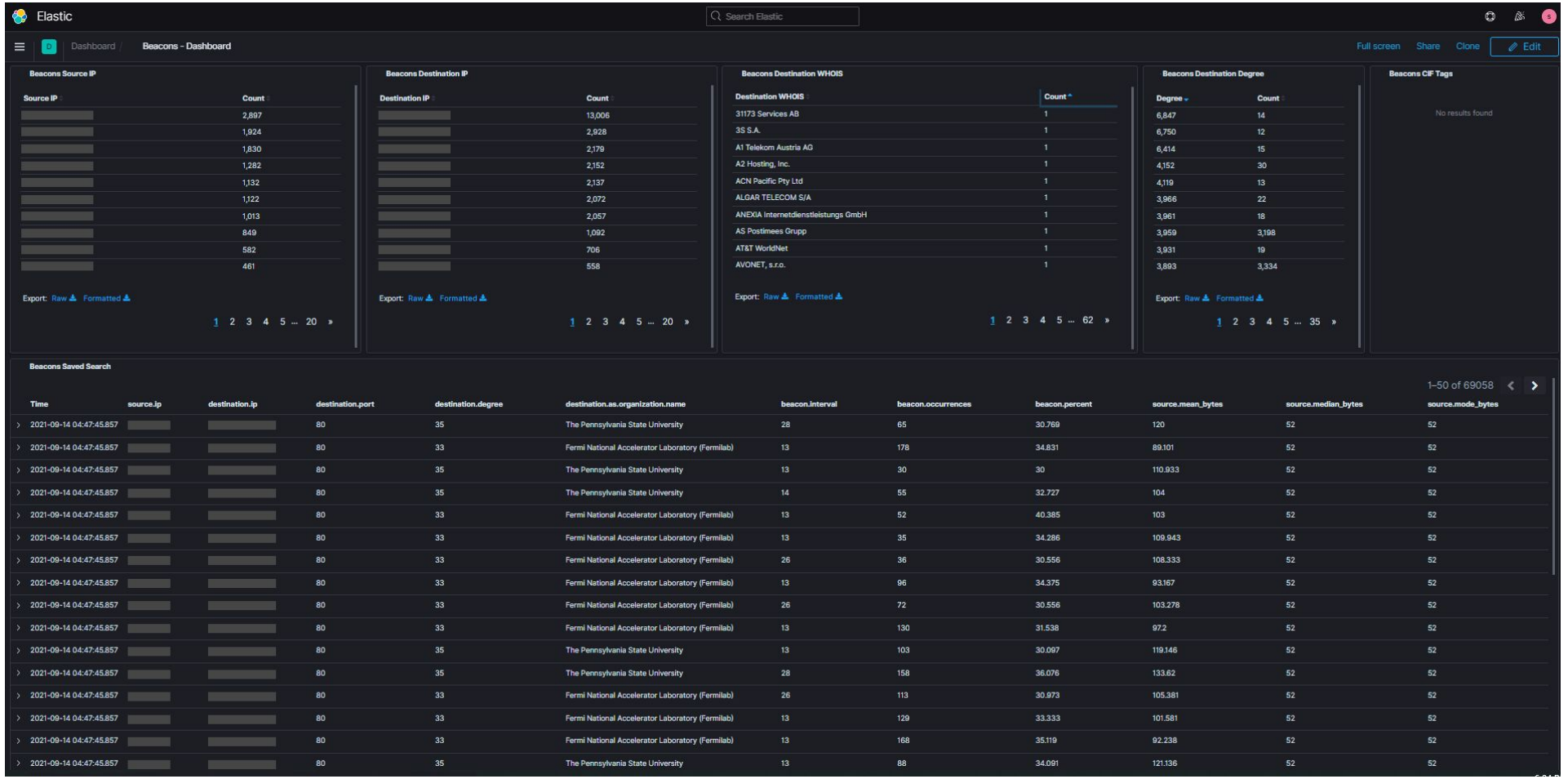


Malware automated detection



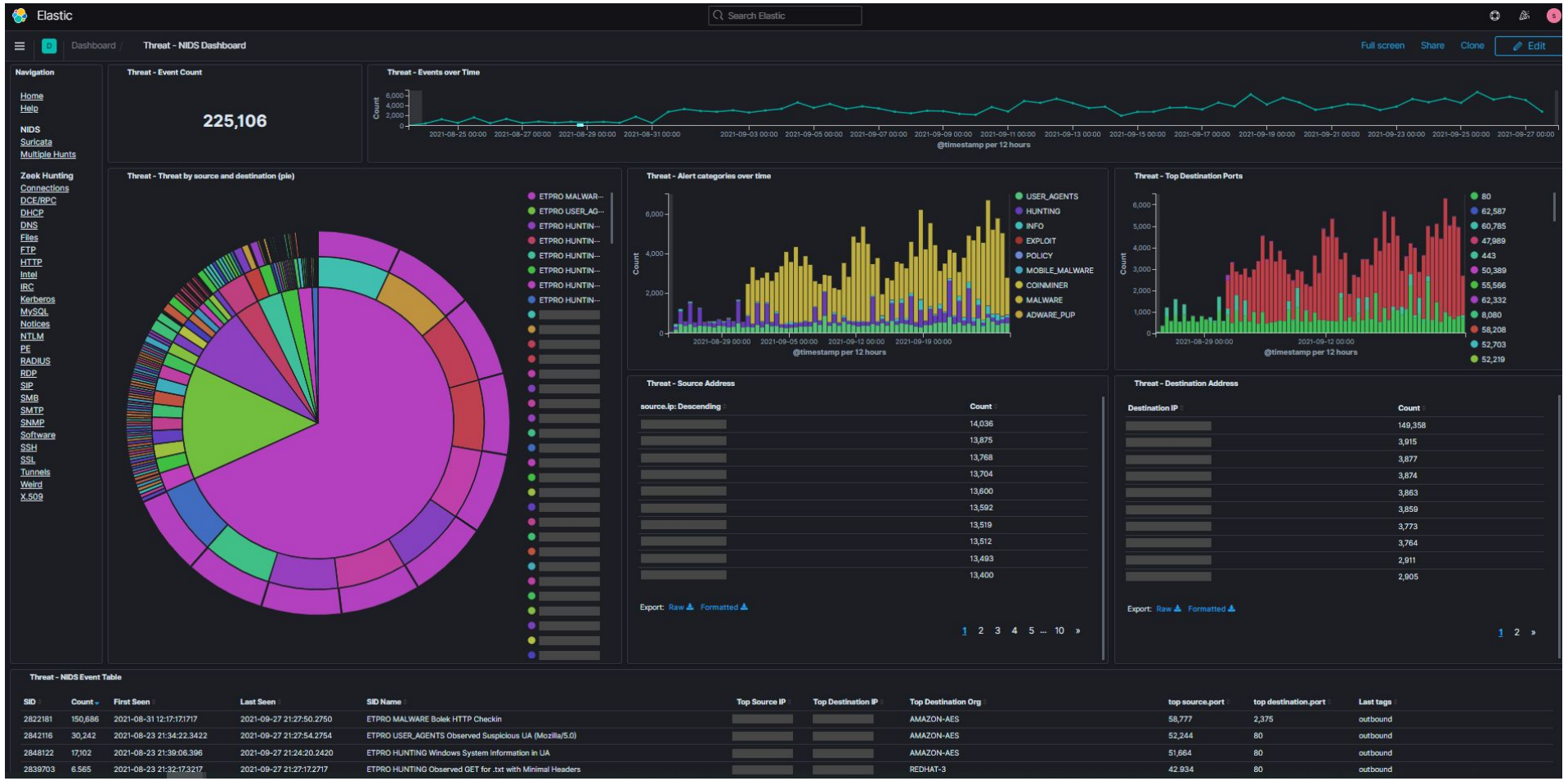
OmniSOC

Flare C2 beacon dashboard



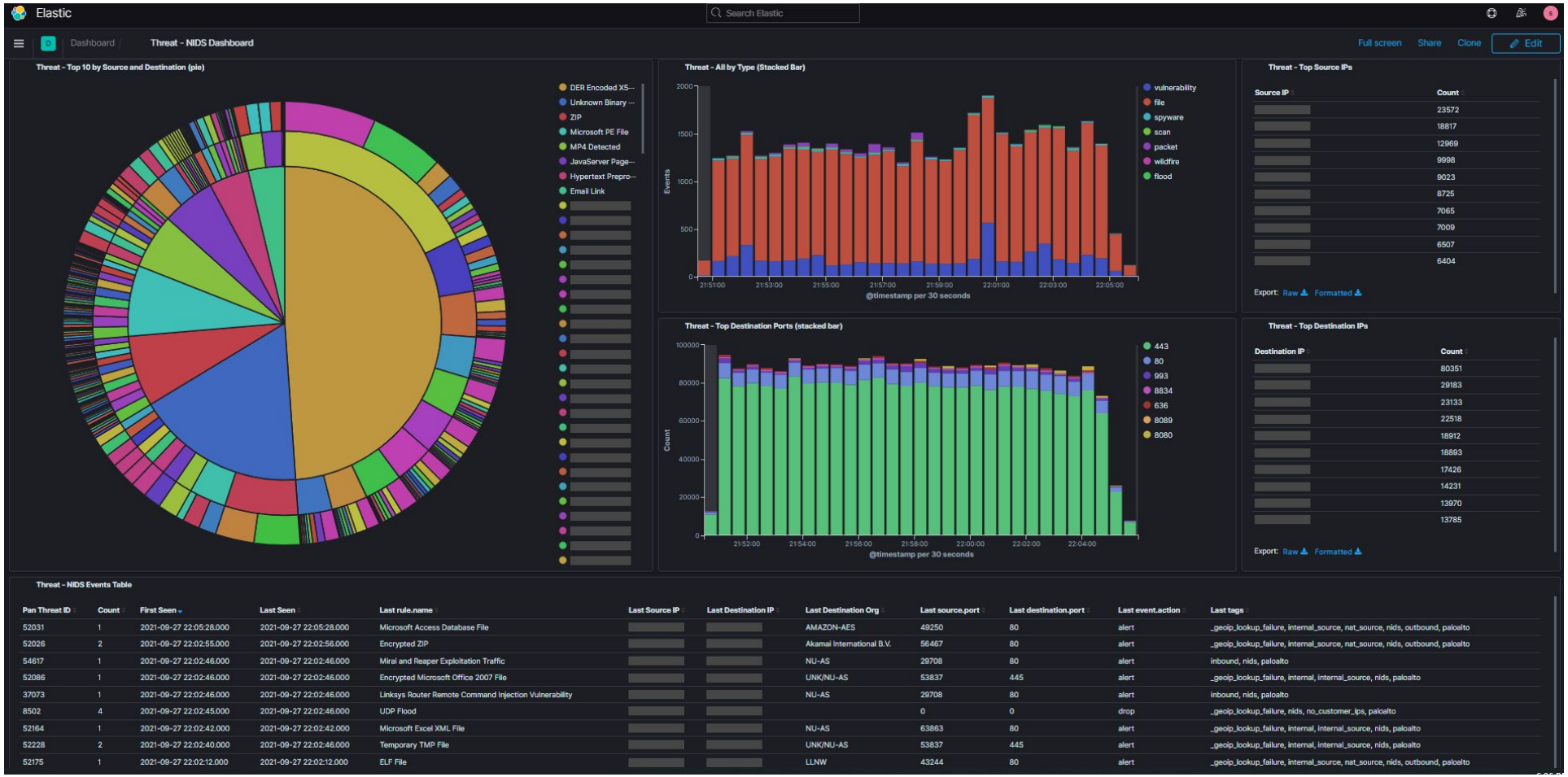
OmniSOC

Suricata NIDS dashboard



OmniSOC

Palo Alto threat dashboard



OmniSOC