24x7x365 Security Operations Monitoring

VIRGINIA TECH™

Partnering with OmniSOC to augment our SOC

OmniSOC was founded by members of the Big Ten Academic Alliance to reduce the time from first detection of a security threat to campus mitigation. Today, our members include higher education and research institutions of all sizes, both public and private. Through ResearchSOC, OmniSOC supplies cybersecurity for the nation's greatest research.

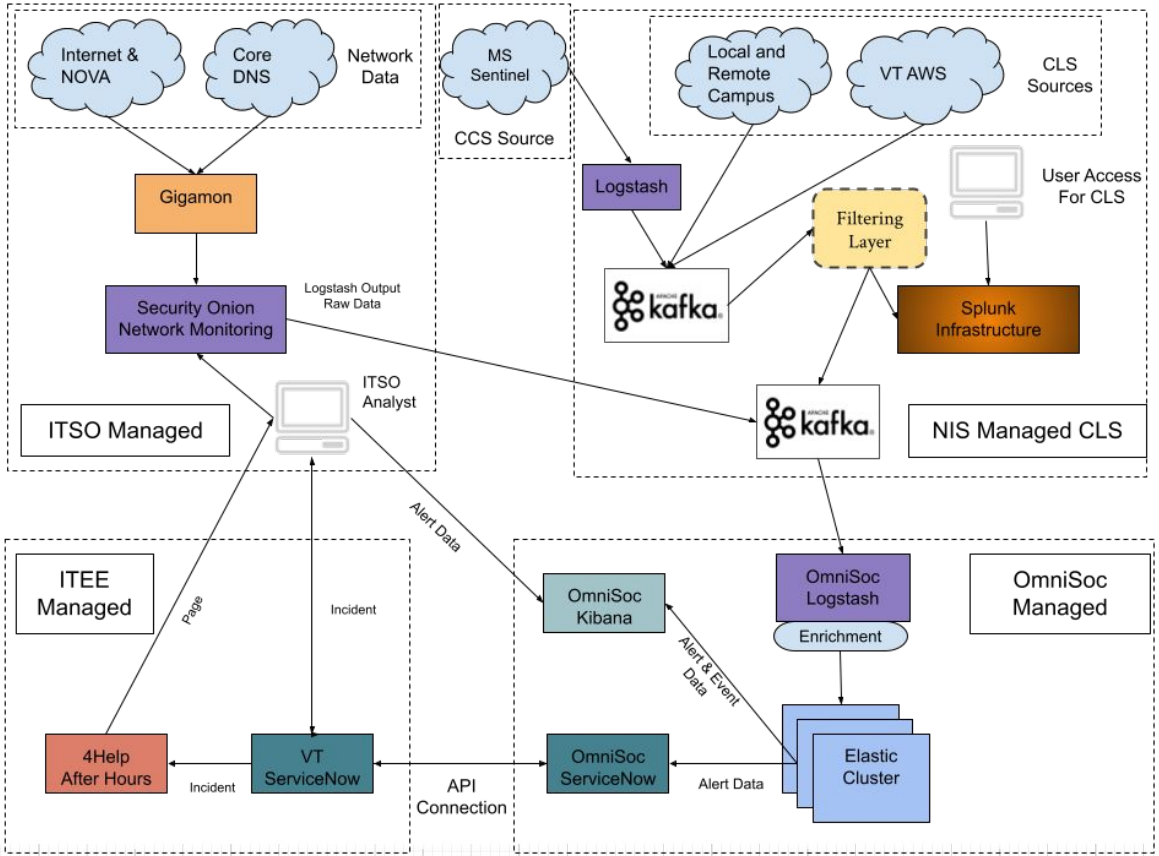
OmniSOC is a part of the Indiana University cybersecurity community (leading.iu.edu), which includes REN-ISAC and the Center for Applied Cybersecurity

VIRGINIA TECH

OmniSOC data

- Zeek connection logs from the edge traffic using Security Onion - ITSO
- Suricata IDS logs from the edge traffic using Security Onion - ITSO
- Zeek DNS logs from edge traffic and core traffic to main NIS servers using Security Onion - ITSO
- Windows Security event logs - CLS
- ITSO is currently working with CCS and CLS to send MDE alerts
- Currently ingesting 1.27 TB/day at OmniSOC (1.5 TB/day contracted)

VIRGINIA TECH


Internet & NOVA
Core DNS
Network Data
MS Sentinel
CCS Source
Local and Remote Campus
VT AWS
CLS Sources
Gigamon
Logstash
User Access For CLS
Filtering Layer
kafka
Security Onion Network Monitoring
Logstash Output Raw Data
Splunk Infrastructure
ITSO Analyst
ITSO Managed
kafka
NIS Managed CLS
Alert Data
ITEE Managed
Page
Incident
OmniSoc Kibana
OmniSoc Logstash
Enrichment
OmniSoc Managed
Alert & Event Data
4Help After Hours
Incident
VT ServiceNow
API Connection
OmniSoc ServiceNow
Alert Data
Elastic Cluster

Security Alerts vs. Incidents in ServiceNow

- Security Alerts - 30 days
  - IDS: 6+ million alerts
  - Conn logs: 8+ billion connections
  - DNS logs: 6+ billion queries
- Incidents created from that data - 30 days
  - 16 incidents dealing with medium or high rated issues
  - 6 created by OmniSOC
    - None after hours (3 were after hours in February)
    - None involved with machines storing high risk data

Go live with 24x7x365 monitoring and response

- Starting tonight, March 31st ITSO will be on call
- Incidents routed through 4help after hours, weekends and holidays
- ITSO paged through OpsGenie
- Vet the incidents
- Identify and notify the responsible parties
- Respond to incident by isolating from network until next business day

What's next?

- ISORA data gives us access to risk levels as well as information about critical priority assets identified in each department
- ITSO will be contacting departments to develop response plans for those critical priority assets to ensure timely response
  - Please respond to incidents and calls as soon as possible
- ITSO will be updating response frameworks we've developed in coordination with the VT Critical Incident Response (CIRT) plan
- Will continue to add data feeds to the OmniSOC ingestion as capacity allows