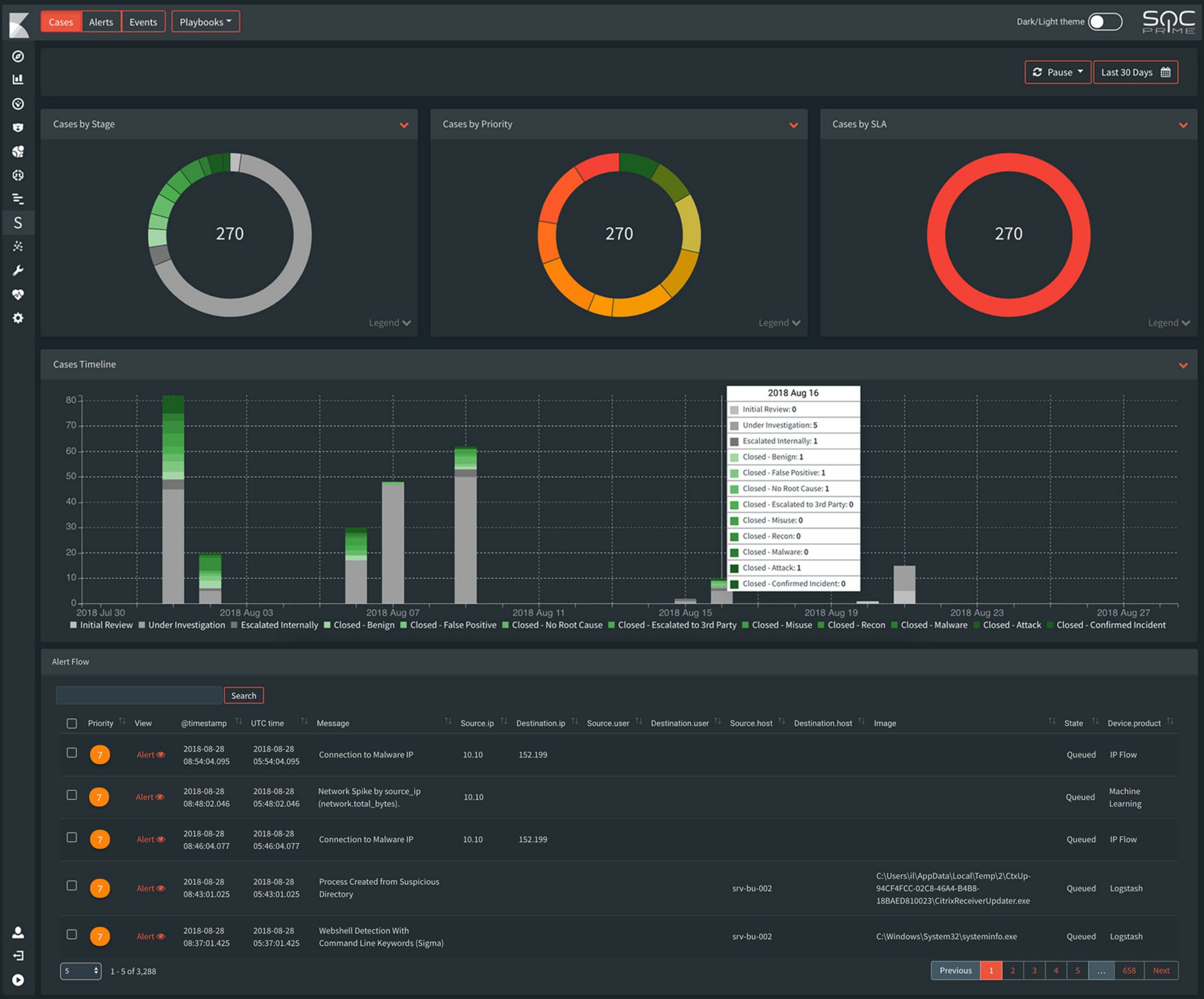
SOC PRIME
SECURITY QUALITY CONTROL

SOC Workflow App

The open-source native Elastic stack SOAR application built to enable collaboration and unleash potential of every analyst on the SOC and Threat hunting team. Unlock the capabilities for the intelligence-powered real-time cyber defense.



□	Priority	View	@timestamp	UTC time	Message	Source.ip	Destination.ip	Source.user	Destination.user	Source.host	Destination.host	Image	State	Device.product
□	7	Alert	2018-08-28 08:54:04.095	2018-08-28 05:54:04.095	Connection to Malware IP	10.10	152.199						Queued	IP Flow
□	7	Alert	2018-08-28 08:48:02.046	2018-08-28 05:48:02.046	Network Spike by source_ip (network.total_bytes).	10.10							Queued	Machine Learning
□	7	Alert	2018-08-28 08:46:04.077	2018-08-28 05:46:04.077	Connection to Malware IP	10.10	152.199						Queued	IP Flow
□	7	Alert	2018-08-28 08:43:01.025	2018-08-28 05:43:01.025	Process Created from Suspicious Directory					srv-bu-002		C:\Users\il\AppData\Local\Temp\2\CtxUp-94CF4FCC-02C8-46A4-B4B8-18BAED810023\CitrixReceiverUpdater.exe	Queued	Logstash
□	7	Alert	2018-08-28 08:37:01.425	2018-08-28 05:37:01.425	Webshell Detection With Command Line Keywords (Sigma)					srv-bu-002		C:\Windows\System32\systeminfo.exe	Queued	Logstash

5 1 - 5 of 3,288

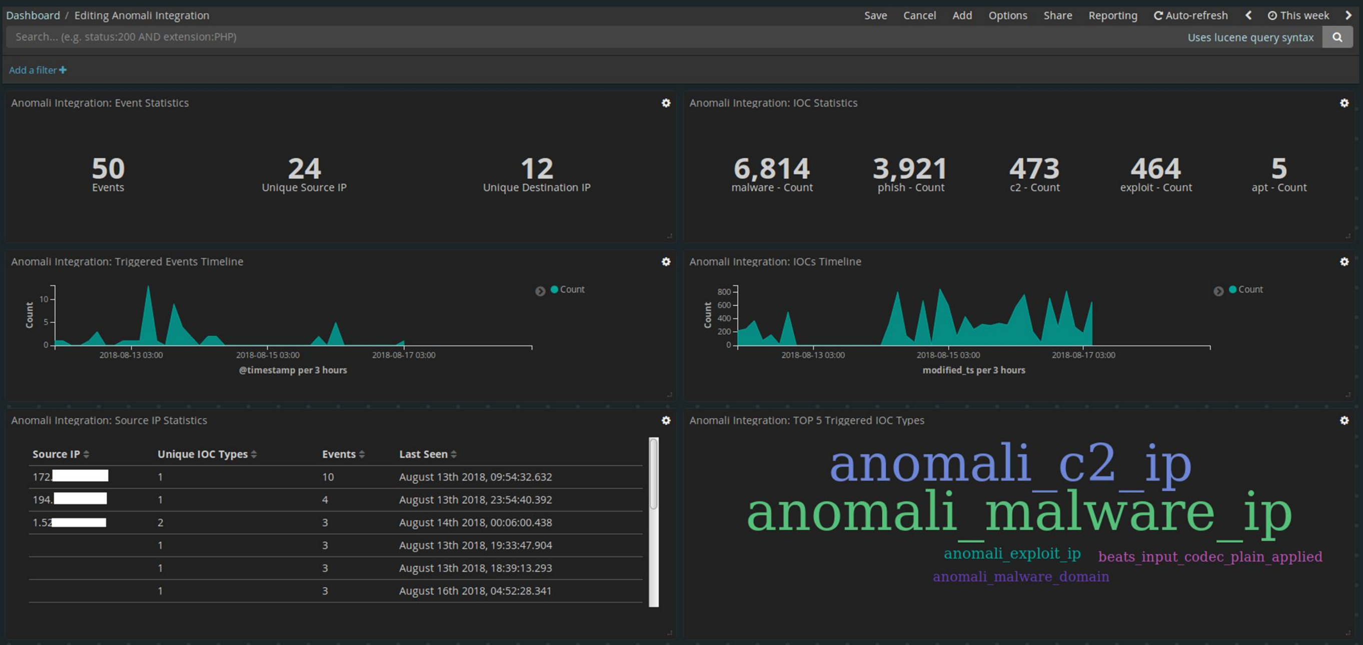
Helps SOC analysts and Threat hunters to carry out investigations based on:

1. Threat Intelligence data enrichments from Anomali ThreatStream & MISP
2. Elastic Machine Learning alerts
3. Saved Searches saved by teammates
4. Assigned hypothesis tests “this IP looks suspicious, see what you can dig up on that”
5. Sigma rules hits on logs, just like Yara for files and Snort for IDS
6. Alerts from SIEM, EDR, IDS arriving at Elastic stack
7. Raw events arriving at Elastic stack
8. Alerts generated automatically by ELK playbooks

☎ 888.484.7555
+44.203.769.3384
sales@socprime.com
socprime.com

Unlimited capabilities & full transparency with open-source Machine Learning

- Complete deployment on Elastic stack with no cloud or new software needed or proprietary code to worry about
- Allows real-time collaboration of multiple analysts on same case
- Every action taken is fully logged and goes back to Elasticsearch database
- Acquired data used for Machine Learning models and feedback system
- Alerts natively supported by X-pack Watcher
- Data fully accessible via Elasticsearch API for integration and playbooks
- Drilldowns in 1-click both to internal data points as well as external systems
- Integration with community-powered Sigma rules, cyber playbooks and incident response actions



Anomali Integration: Event Statistics

50 Events

24 Unique Source IP

12 Unique Destination IP

Anomali Integration: IOC Statistics

6,814 malware - Count

3,921 phish - Count

473 c2 - Count

464 exploit - Count

5 apt - Count

Anomali Integration: Triggered Events Timeline

Anomali Integration: IOCs Timeline

Anomali Integration: Source IP Statistics

Source IP	Unique IOC Types	Events	Last Seen
172.[redacted]	1	10	August 13th 2018, 09:54:32.632
194.[redacted]	1	4	August 13th 2018, 23:54:40.392
1.52[redacted]	2	3	August 14th 2018, 00:06:00.438
	1	3	August 13th 2018, 19:33:47.904
	1	3	August 13th 2018, 18:39:13.293
	1	3	August 16th 2018, 04:52:28.341

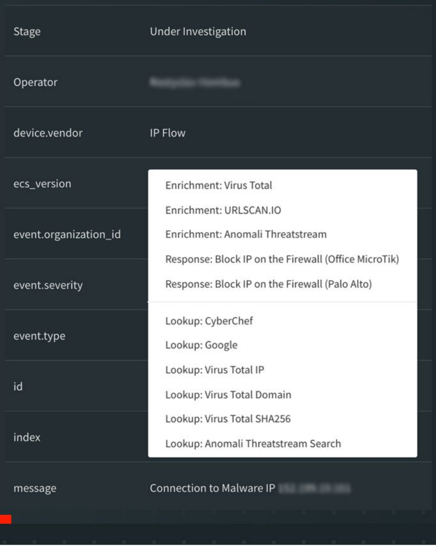
Anomali Integration: TOP 5 Triggered IOC Types

Always up to date on threat intelligence and detection content

- All data is enriched at ingestion with intelligence from Anomali ThreatStream.
- Integration stack is built using the ThreatStream REST API and regularly pulls list of latest IOCs to Logstash dictionaries for the data enrichment during ingestion.
- Continuous detection rules updates from SOC Prime Threat Detection Marketplace
- Automatic matching for C2 IP, Malware IP, Phishing, APT, URL, Domain and Hash.

Simply one interface for the Blue Team

Enrich cyber observables, pivot to hunting tools and respond to the incident: all from the same console using native Kibana UI



Stage	Under Investigation
Operator	[redacted]
device.vendor	IP Flow
ecs_version	
event.organization_id	
event.severity	
event.type	
id	
index	
message	Connection to Malware IP [redacted]

Enrichment: Virus Total
Enrichment: URLSCAN.IO
Enrichment: Anomali Threatstream
Response: Block IP on the Firewall (Office MicroTik)
Response: Block IP on the Firewall (Palo Alto)

Lookup: CyberChef
Lookup: Google
Lookup: Virus Total IP
Lookup: Virus Total Domain
Lookup: Virus Total SHA256
Lookup: Anomali Threatstream Search

888.484.7555
+44.203.769.3384

sales@socprime.com

socprime.com