Overview

Reduce risk
- Security analytics
- Agentless device-level behavior analysis
- Proactive thresholding and alerting
- User accountability

Enrich data context
- Metadata correlation
- SSL decryption data for cloud visibility
- DNS inspection
- URL/URI information

Scale and speed
- Fast reporting
- Millions of flows per second
- Drag-and-drop filtering
- Multi-tenancy

Rapid incident response
- Network as a sensor
- Data you need when you need it most

Scrutinizer: Delivering better security analytics for faster incident response

For decades, and as a best practice, companies have purchased point security products in the name of prevention. Today's growing threat surfaces coupled with the sophistication of attacks has, however, led us to a point where breaches are now inevitable. From the boardroom to the security operations team, organizations must change their mindset away from prevention toward data forensics in support of fast and accurate incident response.

Reduce Risk

The primary security objective for organizations of all sizes is to reduce risk. Products aimed at prevention continue to be part of the equation, but in today's threat environment, the greatest risk reduction occurs from a focus on improving time to resolution after a breach.

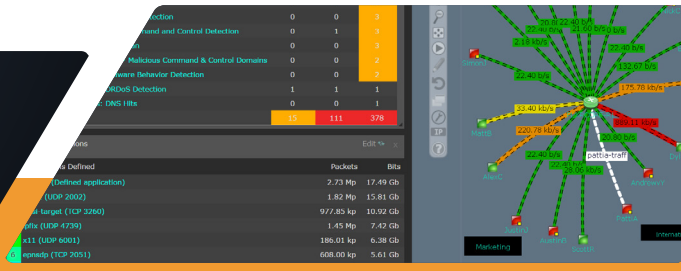
"Bad" things will happen; it is inevitable. In order to reduce risk, you must have a combination of strong forensic data, detailed context, and powerful reporting. These capabilities are the foundation of an effective incident response process.

Enrich Data Context

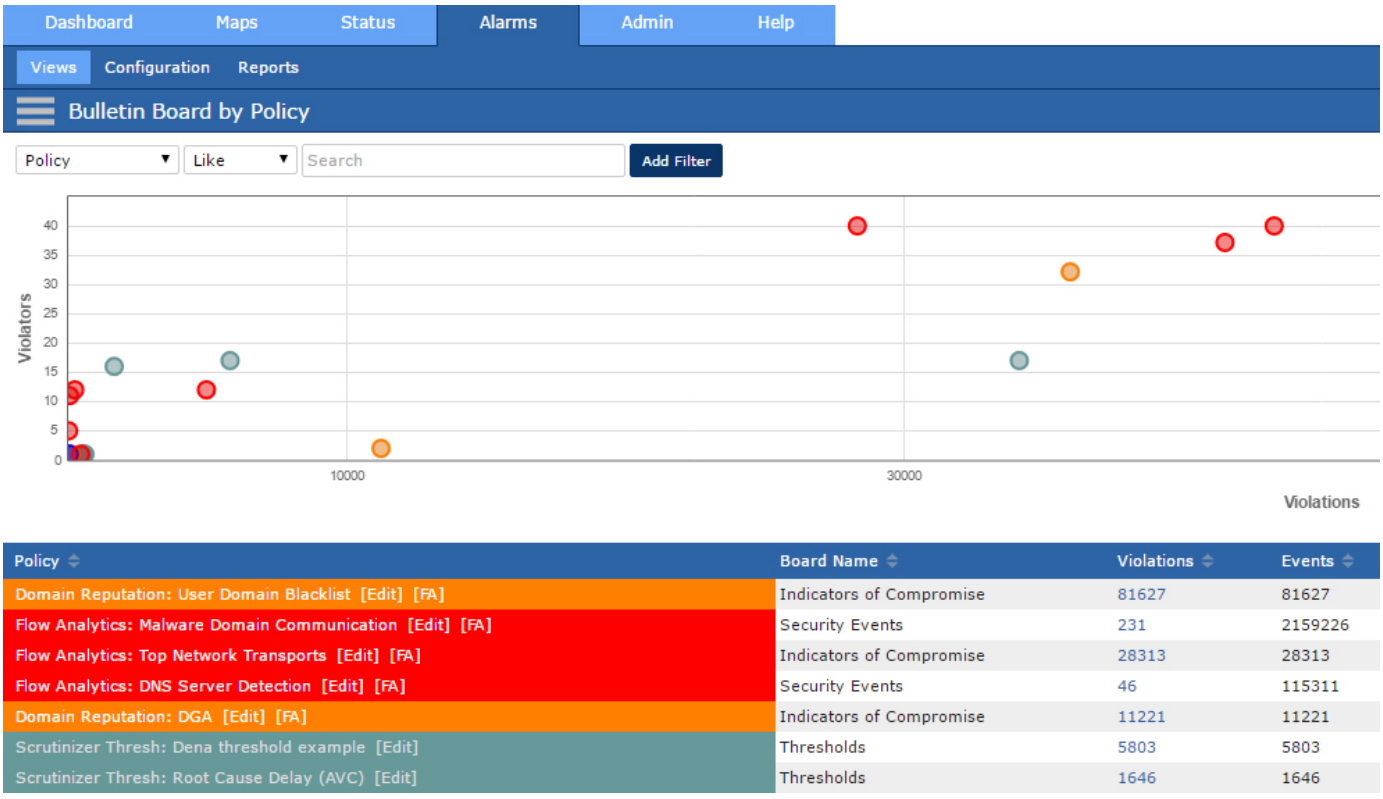
Access to high volumes of raw data does not lead to faster response. In fact, it can have the opposite effect, increasing complexity and slowing response times. What is needed is context and data correlation.

Many systems on the market gather lots of data points, but don't provide context to make the data useful. If you have, for example, a list of Tor connections on your network, but don't know which users accessed those nodes, how useful is the data?

The best context comes from the correlation of network-related data with metadata from point security products like firewalls, IDS/IPS, SIEM, and distributed probes. Everything that runs your business flows across the network. It passes all traffic between users and the applications they need to be productive and drive revenue. Root cause analysis is best derived when you can instantly stitch together the user, device, location, protocol, and application data (including URL and URI) for every flow on the network.



plixer



Policy	Board Name	Violations	Events
Domain Reputation: User Domain Blacklist [Edit] [FA]	Indicators of Compromise	81627	81627
Flow Analytics: Malware Domain Communication [Edit] [FA]	Security Events	231	2159226
Flow Analytics: Top Network Transports [Edit] [FA]	Indicators of Compromise	28313	28313
Flow Analytics: DNS Server Detection [Edit] [FA]	Security Events	46	115311
Domain Reputation: DGA [Edit] [FA]	Indicators of Compromise	11221	11221
Scrutinizer Thresh: Dena threshold example [Edit]	Thresholds	5803	5803
Scrutinizer Thresh: Root Cause Delay (AVC) [Edit]	Thresholds	1646	1646

Figure 1. The Alarms Tab displays a heat map of security events. Network and metadata correlation enables security event prioritization with policy violation details only a click away.

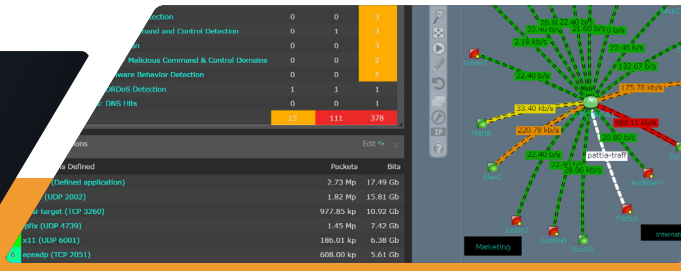
Through partnerships and technology integrations with companies like Cisco, Juniper, Gigamon, Ixia, Palo Alto Networks, Citrix, VMware, Extreme Networks, Endace, Splunk (and many others), Scrutinizer™ provides the data you need for fast and accurate incident response.

Scale and Speed

Even when you have data context available, if the system that houses the data doesn't scale or isn't fast enough to quickly deliver reports, it can't be relied upon in the greatest time of need.

Scrutinizer scales to millions of flows per second through resilient hierarchical deployments, enabled streamlined and efficient data collection. Navigating quickly to the information you need and industry-leading reporting speed are market differentiators for Scrutinizer, ensuring that the information you need is only a few clicks and moments away.

plixer



207.324.8805