BRICATA® | DATA SHEET

Next Generation Intrusion Prevention

A specialized, component-based approach to today's advanced attacks leaves organizations with a stack of tools to manage, lack of visibility across the network, and inconsistent security policies. As threat actors continue to evade detection, your organization's security depends on a responsive approach to new threats and tactics and the ability to hunt for the unknown and targeted threat.

All-In-One Cyber Defense

Bricata is the only solution to combine micro-second malware analysis, next generation IDS/IPS, enriched network metadata, and full packet capture into a single platform, enabling you to achieve total visibility while reducing time to containment and operating costs. Bricata's next generation IPS platform combines three advanced systems to deliver the ultimate protection for your network:

1. Optimized Signature Engine

- More rules across faster connections to see more, stop more
- Multiple threat intelligence sources
- Optimized for modern hardware

2. Malware Conviction Engine

- Near real-time conviction of zero-day malware
- Cylance-patented algorithms and machine learning
- "In-box" and "on-prem" analysis

3. Network Behavior Engine

- Capabilities to detect anomalies that are impossible using standard rules
- Powerful hunting workflows to find threats hiding in the network
- Enriched metadata for alerts generated by Snort rules or binary analysis

True Next Generation IPS

Bricata takes advanced threat protection to a new level, integrating optimized detection, contextual awareness, and extensible and continuous network behavior monitoring and analytics.

Detect & Prevent What Other Solutions Miss

The alarming truth is that legacy IDS is ineffective. A dependence on signatures, limited rule sets, and outdated architecture can't provide the real-time protection necessary to defend against the current generation of advanced threats. Relying on them can expose your organization to devastating breaches.

THE BRICATA SOLUTION

UNPARALLELED DETECTION

- **Optimized Signature Engine:** See more, stop more
- **Malware Conviction Engine:** Outpaces sandbox technology, accelerates response, shortens time to containment
- **Network Behavior Engine:** Delivers metadata enriched alerts, detects attacks that legacy IDS/IPS can't
- Full landscape visibility, extended with full packet capture
- Identify anomalies with extensible, continuous monitoring and analytics

A STRENGTHENED SECURITY ECOSYSTEM

- Control over your deployment with sophisticated policy management
- Customize detection and decrease false positives with flexible policy tuning
- Extend the value of investments by sharing event data with existing SIEM and analytics tools

Bricata's takes advantage of multi-threaded and multi-processor systems to deliver greater performance and better detection, because you can't protect what you can't detect.

Accelerate Response, Shorten Time to Containment

Increased complexity and frequency of attacks elevate the need for rapid response and speed to resolution. While many solutions rely upon integration with external sandbox-based solutions to identify malware, Bricata identifies malware in near real-time. Powered by the same machine learning-based detection that powers Cylance, Bricata allows you to respond faster, reduce dwell time, and shorten time to containment.

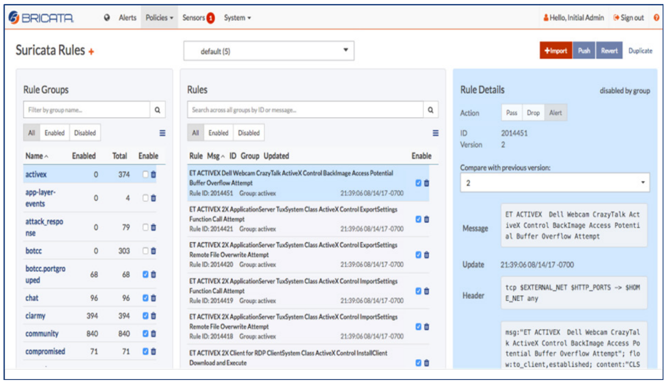
Stop Ongoing Attacks with Real-Time Contextual Awareness

Determining if alert escalation is necessary must be correct every time. Unfortunately, most security teams are deluged with alerts and have little context to distinguish genuine threats from noise.

Bricata's customizable network behavior engine delivers enriched metadata to provide context around alerts, extending your visibility beyond simple alert data to provide a broad view of behavior around targeted systems.

Go On the Hunt for Hidden Threats

Advanced cyber threat actors penetrate networks in ways that fly below the radar of existing security technologies. Once in, they expand their access privileges across the network and introduce additional malware, creating hidden threats and maintaining a persistent presence.



Suricata Rules +

default (5)

Rule Groups

Filter by group name...

Name ^	Enabled	Total	Enable
activex	0	374	☐
app-layer-events	0	4	☐
attack_response	0	79	☐
botcc	0	303	☐
botcc.portgrouped	68	68	☑
chat	96	96	☑
ciarmy	394	394	☑
community	840	840	☑
compromised	71	71	☑

Rules

Search across all groups by ID or message...

Rule Msg ^ ID Group Updated	Enable
ET ACTIVEX Dell Webcam CrazyTalk ActiveX Control BackImage Access Potential Buffer Overflow Attempt Rule ID: 2014451 Group: activex 21:39:06 08/14/17 -0700	☑
ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ExportSettings Function Call Attempt Rule ID: 2014421 Group: activex 21:39:06 08/14/17 -0700	☑
ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ExportSettings Remote File Overwrite Attempt Rule ID: 2014420 Group: activex 21:39:06 08/14/17 -0700	☑
ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ImportSettings Function Call Attempt Rule ID: 2014419 Group: activex 21:39:06 08/14/17 -0700	☑
ET ACTIVEX 2X ApplicationServer TuxSystem Class ActiveX Control ImportSettings Remote File Overwrite Attempt Rule ID: 2014418 Group: activex 21:39:06 08/14/17 -0700	☑
ET ACTIVEX 2X Client for RDP ClientSystem Class ActiveX Control InstallClient Download and Execute	☑

Rule Details disabled by group

Action: Pass Drop [✓ Alert]

ID 2014451

Version 2

Compare with previous version: 2

Message

```
ET ACTIVEX  Dell Webcam CrazyTalk Act
iveX Control BackImage Access Potenti
al Buffer Overflow Attempt
```

Update 21:39:06 08/14/17 -0700

Header

```
tcp $EXTERNAL_NET $HTTP_PORTS -> $HOM
E_NET any
```

```
msg:"ET ACTIVEX  Dell Webcam CrazyTal
k ActiveX Control BackImage Access Po
tential Buffer Overflow Attempt"; flo
w:to_client,established; content:"CLS
```

Optimize rule performance, integrate tactical threat intelligence, minimize false positives, and focus on only the most important alerts with rules where and how you need them.

Bricata records file and network activity on the endpoint and provides enhanced forensic data to better equip security teams to identify malicious behavior — including anomalous device communication, command and control activity, and lateral movement — and hunt for threats hiding inside the network.

Establish Continuous Monitoring

Bricata provides extensible, continuous monitoring, allowing you to define, collect, and archive baseline metadata. Use this to better characterize how network assets interact and facilitate real-time and investigate retroactively when new types of attacks or new types of communications are discovered.

Streamline Operations, Reduce Complexity, Reduce Costs

Other solutions ignore the legacy or unique components of the security infrastructure. Bricata federates all of your network security components to automate and streamline operations with the most effective, affordable solution for situational awareness, advanced threat detection and analysis, and proactive threat defense.

DETECTION.

Compound, optimized detection engine

VISIBILITY.

Extensible, continuous network behavior monitoring and analytics

SECURITY ECOSYSTEM STRENGTH.

Threat intelligence exchanged with your environment, leveraging open source