Cloud Platform Evolution

Growing portfolio with 19+ apps
Cloud Agent driving product adoption
Organically built multi-petabyte data lake

Better cross-product and third-party data correlation...
Data Lake and Security Analytics Goals

Provide a coherent and actionable view of your security posture by breaking down security data silos

Coalesce all data into a centralized highly scalable security data lake

Combine and enrich Qualys generated findings with third party signals

Leverage the strength of Qualys Cloud Platform, Cloud Agent and Apps to build a comprehensive security analytics platform
Security Analytics Use Cases

- Real-time streaming correlation and analytics with out-of-box rules
- Out-of-band batch analytics over historical data
- Ad-hoc querying and threat hunting on enriched and security aware data sets
- Advanced analytics use cases using machine learning
- Orchestration with playbooks
- Response and endpoint protection
Advanced Correlation and Analytics

ML/AI Service
Patterns | Outlier | Predictive SoC

Orchestration & Automation
Integration | Playbooks | Response

UEBA
User & Entity Behavior Analytics

Threat Hunting
Search | Exploration | Behavior Graph

Security Analytics
Anomaly | Visualization | Dashboard

Advanced Correlation
Actionable Insights | Out-of-box Rules

Qualys Security Data Lake Platform
Data Ingestion | Normalization | Enrichment | Governance

Qualys Quick Connectors

Qualys Apps
CA | VM | AI | PC | IOC | WAS | WAF

Network | Firewall | Server | End Point

Apps | Cloud | Users | IoT
Correlation and Data Platform Architecture

Qualys Apps
- CA
- VM
- AI
- WAS
- PC
- IOCs
- FIM
- PM
- WAF
- PCI
- CS
- CI

Third Party Sources
- Apps
- Firewall
- Users
- IoT
- Cloud
- IPS

Qualys Streaming Data Backbone

Normalization and Enrichment

Real-time Stream Processing

Batch Processing

Security Data Lake
- Hadoop
- elastic
- cassandra
- JanusGraph
- Amazon S3

Machine Learning

Visualization

Threat Hunting

Orchestration Automation

APIs
Threat Actor targets webserver with known vuln CVE-2018-7600 (Drupalgeddon2).

Threat Actor:
- Steals credential by using Mimikatz and logs into domain controller.

IDS Logs Attempted Exploit

IOC detects post exploit tool, correlate to Mimikatz

Cloud Agent Detects & Log Login activity

CVE Exploited Emergency Patch applied

Passive Sensor Logs outbound C&C traffic

IT Infra Events

Security Infra Events

Continuous Logging from Qualys Apps and 3rd Party

Correlation Engine

Threat Storyline

SOAR

Next-Gen Analytics, Data Lake and Orchestration

Behavioral Analytics across MITRE ATT&CK stages

Threat Actor:
- Could NOT exfiltrate the sensitive info.

SOC Analyst Can stop attacks before data exfiltration

Threat Actor:
- Could NOT exfiltrate the sensitive info.

Cloud Agent Detects & Log Login activity

Passive Sensor Logs outbound C&C traffic

IDS Logs

Attempted Exploit

Initial Access

Execution

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Exfiltration

C&C

MITRE ATT&CK Stages

Qualys

Threat Actor targets webserver with known vuln CVE-2018-7600 (Drupalgeddon2). Threat Actor:
- Steals credential by using Mimikatz and logs into domain controller.

IDS Logs Attempted Exploit

IOC detects post exploit tool, correlate to Mimikatz

Cloud Agent Detects & Log Login activity

CVE Exploited Emergency Patch applied

Passive Sensor Logs outbound C&C traffic

IT Infra Events

Security Infra Events

Continuous Logging from Qualys Apps and 3rd Party

Correlation Engine

Threat Storyline

SOAR

Next-Gen Analytics, Data Lake and Orchestration

Behavioral Analytics across MITRE ATT&CK stages

Threat Actor:
- Could NOT exfiltrate the sensitive info.

SOC Analyst Can stop attacks before data exfiltration

Threat Actor:
- Could NOT exfiltrate the sensitive info.

Cloud Agent Detects & Log Login activity

Passive Sensor Logs outbound C&C traffic

IDS Logs

Attempted Exploit

Initial Access

Execution

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Exfiltration

C&C

MITRE ATT&CK Stages

Qualys
### Event Source Catalog

Apps help you get started gaining insights from your data source by providing example searches and dashboards for common use cases. Feel free to edit them as you need to get the results you want.

<table>
<thead>
<tr>
<th>Event Source</th>
<th>Configured</th>
<th>Mar 12, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Palo Alto Firewall</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Salesforce Cloud Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Palo Alto Firewall</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0365 Cloud Services</strong></td>
<td>Coming Soon</td>
<td></td>
</tr>
<tr>
<td>ORadar SIEM</td>
<td>Coming Soon</td>
<td></td>
</tr>
<tr>
<td><strong>Qualys VM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Qualys Log Collector</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Microsoft AD</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Splunk SIEM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tipping Point</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WAF</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WAF</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DDoS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web Proxy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Decoy/Deception</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security Analytics – Milestone Timelines

- **Nov 2019 – Milestone 1**
  - Demo at QSC
  - Adv Correlation Engine

- **April 2020 – Milestone 2 (Alpha)**
  - Adv Correlation Engine
  - MITRE ATT&CK Analytics
  - Connector Library

- **Aug 2020 – Milestone 3 (Beta)**
  - SIEM Connectors
  - Incident Response
  - Real-Time Context Enrichment
  - Alert Triage, Investigation & Prioritization

- **Nov 2020 – Milestone 4 (GA)**
  - UEBA, Threat Hunting
  - Data Analytics
  - 50+ Connector Library
Thank You

Dilip Bachwani
dbachwani@qualys.com