Cisco Stealthwatch for MSSPs: Security Analytics Services without upfront cost or risk

Crystal Moody
Sr. Product Manager
December 2018
Today’s Presenters

John Malzahn
Senior Manager, Service Provider Solutions Marketing
Cisco Systems

Crystal Moody
Product Manager, Cisco Stealthwatch
Cisco Systems
Agenda

1. Market Needs
2. Stealthwatch Cloud Product Overview
3. How it Works
4. Packaging for Managed Service Providers
5. Take the Next Step to Learn More
Businesses of all sizes need to be thinking about security

- **$7M** was the average cost per breach in the U.S. in 2017
- **55%** of SMBs with under 1,000 employees experienced cyberattacks in the last year
- **52%** of cyber attack victims in 2016 haven’t made changes in 2017
- **30%** of SMBs consider regulatory and compliance constraints as high security risks

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
But most security solutions require significant investment

- Upfront capital investment
- Added complexity
- Dedicated security staff & continuous training
- Ongoing management costs
- Extended deployment time
Effective security depends on visibility and understanding

- KNOW every host
- RECORD every conversation
- Understand what is NORMAL
- Be alerted to CHANGE
- Respond to THREATS quickly

Effective security depends on visibility and understanding. To ensure security, it is crucial to know every host, record every conversation, understand what is normal, be alerted to any changes, and respond to threats quickly.
Automated threat analytics across on premises and cloud networks
Monitor and understand behavioral data over time

*Dynamic Entity Modeling*

**Collect Telemetry**
- IP Meta Data
- System Logs
- Security Events
- Passive DNS
- External Intel
- Vulnerability Scans
- Config Changes

**Perform Analysis**
- Role
- Group
- Consistency
- Rules
- Forecast

**Draw Conclusions**
- What is the role of the entity?
- What ports/protocols does the entity continually access?
- What connections does it continually make?
- Does it communicate internally only?
- What countries does it talk to?
- How much data does the device normally send/receive?
Is Stealthwatch Cloud helpful?

Was this alert helpful?
This provides feedback to us. It doesn’t directly change our alerting criteria.

Yes No

Snooze this alert?

<table>
<thead>
<tr>
<th>Type</th>
<th>Scope</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excessive Access Attempts (External)</td>
<td>Source</td>
<td>10.3.0.2</td>
</tr>
</tbody>
</table>

Don’t show the alert matching the above criteria for a period of:

Don’t snooze

<table>
<thead>
<tr>
<th>Was this helpful?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1 2017</td>
<td>94%</td>
</tr>
<tr>
<td>Q2 2017</td>
<td>97%</td>
</tr>
<tr>
<td>Q3 2017</td>
<td>95%</td>
</tr>
<tr>
<td>Q4 2017</td>
<td>94%</td>
</tr>
<tr>
<td>Q1 2018</td>
<td>94%</td>
</tr>
<tr>
<td>Q2 2018</td>
<td>95%</td>
</tr>
<tr>
<td>Q3 2018</td>
<td>94%</td>
</tr>
<tr>
<td>Lifetime</td>
<td>95%</td>
</tr>
</tbody>
</table>
Identify every entity in your network automatically

Automated Entity Discovery

Detect

Track

Profile
Understand the function of each entity

*Dynamic Role Tracking*

Roles include:

- Android
- Kerberos Node
- AWS Resource
- Mail Server
- Wireless LAN Controller
- Medical Imaging Client
- Citrix PVS Server
- Remote Desktop Server
- Database Server
- Terminal Server
- DNS Server
- VoIP Client
- Domain Controller
- Legacy Windows Device
- Apple iOS
- Web Server

...and 20+ more
Detailed visibility of every entity

**Automated Entity Tracking**

Time of Day Usage

Traffic Statistics

Active Traffic Profiles
Traffic profiling on every entity

Automated Entity Profiling

Connections by profile

Traffic Statistics by profile
Observations are building blocks for modeling

Automatic event detection

View observations for a specific host

See Observation details
Alerts reference Observations

Automatic event detection

Potential Database Exfiltration

- Postgres-db-01

Status: Open
ID: 566
Description: A statistically unusual amount of data was transferred from a database server to a client.

Updated: Nov 18, 2016 12:02:33 AM
Created: Nov 18, 2016 12:02:33 AM

IPs at the time of alert: 10.0.0.241
Hostname at the time of alert: postgres-db-01

Assignee: Nobody
Tags: 

Supporting Observations

New High Throughput Connection Observation

Device has exchanged a large amount of traffic with a new host.

<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP</th>
<th>Connected IP</th>
<th>Local Connection</th>
<th>In B</th>
<th>Out B</th>
<th>Time Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/11/16 2:13 PM</td>
<td>postgres-db-01</td>
<td>205.255.255.251</td>
<td>no</td>
<td>1,989,982,518</td>
<td>17,967,288,803</td>
<td>5h 38m 51s</td>
</tr>
</tbody>
</table>

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

High throughput to new host

Russia identified as suspicious country
Detect abnormal activity using entity modeling

- IP address detected
- Communicates with set of IPs
- Classify roles: Dynamically assign roles to entities
- Database server identified
- Data stays within environment
- Data access from regular location
- Existing IP accesses database server
- New External Connection observation
- New High Throughput Connection
- 36 Day Baseline Monitor and model behavior
- Alert Triggers for Database Exfiltration
Low-noise alerts help you solve problems

ALERT: Anomaly detected

95% of Stealthwatch Cloud alerts rated as “helpful” by current customers

- Excessive failed access attempts
- DDoS and amplification attacks
- Potential data exfiltration
- Geographically unusual remote access
- Suspected botnet interaction
Full indexing and filtering

<table>
<thead>
<tr>
<th>Session Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by:</strong></td>
</tr>
<tr>
<td><strong>IP</strong></td>
</tr>
<tr>
<td><strong>Connected IP</strong></td>
</tr>
<tr>
<td><strong>Port</strong></td>
</tr>
<tr>
<td><strong>Connected Port</strong></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td><strong>Bytes to</strong></td>
</tr>
<tr>
<td><strong>Packets to</strong></td>
</tr>
</tbody>
</table>

Enter a start date/time and an end date/time for the search. Longer time ranges will take longer to load.

| Start Date | 2017-03-25 |
| Start Time | 00:00 |

Search on any host
Evaluate telemetry against known applications

**Dynamic Entity Modeling**

Easily detect violations to organizational policies
Summary entity reports

### Top Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Bytes Total</th>
<th>B ytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5092/tcp</td>
<td>315,554,795,421</td>
<td></td>
</tr>
<tr>
<td>2260/tcp</td>
<td>315,552,977,438</td>
<td></td>
</tr>
<tr>
<td>22/tcp (telnet)</td>
<td>240,489,694,467</td>
<td></td>
</tr>
<tr>
<td>22/tcp (ssh)</td>
<td>209,568,757,483</td>
<td></td>
</tr>
<tr>
<td>53880/tcp</td>
<td>139,888,037,709</td>
<td></td>
</tr>
<tr>
<td>445/tcp (microsoft-ds)</td>
<td>119,555,466,149</td>
<td></td>
</tr>
<tr>
<td>49158/tcp</td>
<td>118,969,918,573</td>
<td></td>
</tr>
<tr>
<td>443/tcp (https)</td>
<td>115,057,711,229</td>
<td></td>
</tr>
<tr>
<td>49172/tcp</td>
<td>90,021,408,637</td>
<td></td>
</tr>
<tr>
<td>53425/tcp</td>
<td>65,688,032,265</td>
<td></td>
</tr>
</tbody>
</table>

Showing 1 to 10 of 125,445 entries. CSV

### Top IPs

<table>
<thead>
<tr>
<th>IP</th>
<th>Bytes To</th>
<th>Bytes From</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.201.3.25</td>
<td>266,738,786,721</td>
<td>266,484,785,629</td>
<td>2,226</td>
</tr>
<tr>
<td>10.201.1.84</td>
<td>266,045,816,163</td>
<td>1,428,423,963</td>
<td>266,420,362,241</td>
</tr>
<tr>
<td>10.201.8.15</td>
<td>235,395,272,910</td>
<td>95,656,982,524</td>
<td>105,621,679,893</td>
</tr>
<tr>
<td>10.201.3.149</td>
<td>235,162,542,713</td>
<td>233,231,901,549</td>
<td>1,033,542,186</td>
</tr>
<tr>
<td>10.201.3.72</td>
<td>230,278,509,281</td>
<td>2,671,932,228</td>
<td>237,461,771,033</td>
</tr>
<tr>
<td>10.201.3.23</td>
<td>160,185,920,359</td>
<td>94,890,047,394</td>
<td>95,395,672,355</td>
</tr>
<tr>
<td>10.19.30.15</td>
<td>135,096,674,806</td>
<td>70,536,592,736</td>
<td>65,561,373,264</td>
</tr>
<tr>
<td>10.201.8.55</td>
<td>118,973,580,536</td>
<td>59,819,683,686</td>
<td>59,113,864,842</td>
</tr>
<tr>
<td>10.201.3.19</td>
<td>90,448,147,610</td>
<td>90,078,171,366</td>
<td>2,369,978,312</td>
</tr>
<tr>
<td>10.10.33.99</td>
<td>92,900,980,835</td>
<td>62,580,123,312</td>
<td>68,908,236,123</td>
</tr>
</tbody>
</table>

Showing 1 to 10 of 4,144 entries. CSV
Track elastic resource behavior

AWS Lambda
Flexible Security for Dynamic Environments

Stealthwatch Cloud

<table>
<thead>
<tr>
<th>Native Cloud Logs</th>
<th>Premises Network Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon AWS</td>
<td>NetFlow</td>
</tr>
<tr>
<td>Azure</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Google Cloud Platform</td>
<td>Mirror/Span</td>
</tr>
</tbody>
</table>
See all network activity by utilizing existing telemetry sources

*Virtual Sensors*

Use DNS Lookups to link dynamics IPs to a host name

Collect from all these sources
- NetFlow
- DNS
- SIEM
- Active Directory
- IPFIX
- Gigamon
- Any Mirror/SPAN

Stealthwatch Cloud

IP Traffic Data

Other Security Data

Switches
Firewalls
Mirror/Span Ports
Load Balancers
Application Servers
Threat Detection
Amazon Web Services Architecture

- SaaS Portal
- Stealthwatch Cloud
- API
- Role Created for Stealthwatch Cloud in Account
- Permissions allow Stealthwatch Cloud to read AWS services
- Amazon Account
- CloudTrail
- Inspector
- GuardDuty
- Lambda
- Config
- Amazon VPC
- Amazon CloudWatch
Google Cloud Platform Architecture

Stealthwatch Cloud

API

SaaS Portal

Permissions allow Stealthwatch Cloud to read GCP Flow Logs

GCP Account

Stealthwatch Cloud User with permissions

Stackdriver

Virtual Private Cloud

Google Compute Engine
Microsoft Azure Architecture

Stealthwatch Cloud

Permissions allow Stealthwatch Cloud to read NSG Flow Logs

SaaS Portal

API

Role Created for Stealthwatch Cloud in Account

Network Watcher

Virtual Network

Azure Resources

Azure Account

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Empower your team to make informed security decisions

- Keep inventory of every entity on your network
- Prove compliance with organized records
- React to reliable, actionable alerts
- Enhance productivity in existing workforce
- Drive deeper insight with entity modeling
Managed Services Provider Solution
Security challenges are an opportunity for MSSPs

Managed Security Services

Simplicity

Speed
Get complete visibility into tenant networks

See all activity in your tenant’s environment by monitoring all IP-based traffic

Understand security data through automatically organized groups

Know what happened for later investigation informed by continuous activity tracking
Automatically detect threats and indicators of compromise

Monitor activity in real time with telemetry traffic analysis

Establish baseline for normal behavior and identify anomalies over time with entity modeling

Enable smarter response and reduce investigation times with high-fidelity alerts
And get the visibility you need simply and efficiently

Manage from one easy-to-consume SaaS interface with multi-tenant support, built-in analytics, and behavior predictions

Deploy in minutes with minimal setup

Scale effortlessly with automated configuration and device discovery
Case Study

Company profile
Luxembourg-based information technology integrator, cloud, and telecom service provider.

Test Results
“Stealthwatch Cloud was able to pinpoint the needles in the haystack: unusual IPs, traffic to strange countries, denial-of-service attacks, and password brute-force attacks were detected in a test environment.”

Benefits
“The number-one benefit to Stealthwatch Cloud is that it is independent of the hosting environment. We are not just focusing on our clouds, but also enable on-premises and public cloud environment usage. We need something that works in such hybrid environments, which is where our customers need us to be.”
Managed Security Services are in high demand

- Service Providers can leverage Stealthwatch Cloud to deliver security monitoring and threat detection services to their end clients.
  - Managed Security Services (MSS) has projected CAGR of 14.5% from 2016-2022, reaching $45B.¹
  - 44 percent of enterprises and 54 percent of small businesses outsource their security monitoring capabilities.²
  - Stealthwatch Cloud provides the technology platform that will enable IT service providers, among others, to enter the MSS market.

- Stealthwatch Cloud was purpose-built to allow a service provider to manage multiple tenants within the larger cloud-based architecture.

- MSLA delivers a specific approach to agreements and pricing designed to facilitate this business.
Managed Services Licensing Agreements

Cisco sales program designed to meet the specific needs of a Managed Service Provider (MSP/MSSP)

- Provides a consumptive, utility based buying program with shared risk and shared success
  - Designed to promote the service launch and ramp up of the Service Provider’s GTM Lifecycle.

- Post-paid, monthly billing based on actual usage
  - Allows the MSP/MSSP to align services costs with actual services revenues.
  - Lowers the barrier to entry to deliver Managed Security Services by eliminating risk, and reducing upfront capital costs associated with hardware / software.

- License pooling and reuse is accommodated
  - Allowing the service provider to manage customers and account as they need to conduct their business.

- Basic and Premium offering levels encourage quick ramp up and volume commitments
  - When Service Provider commits to higher volumes, they receive preferential pricing.
Enable your business to see, secure, and protect with Cisco cloud security

Stealthwatch Cloud

Public Cloud Visibility
Extend visibility to public and hybrid cloud environments

Cloudlock

Cloud access security brokers (CASB)
Secure users, data, and applications in the cloud

Umbrella

DNS Security
Protect users anywhere they go
Start today with a free 60-day trial

Schedule technical review and demo

Learn more: cisco.com/go/stealthwatch-cloud
For more information

Visit www.cisco.com/go/mssp
or contact your Cisco account representatives
Questions?