MSSP success checklist

Managed Security Service Providers (MSSPs), like any other business, are a factor of its people, process, and product.

When you're starting service with a customer, you're also entering into what you hope is a long-term relationship. Setting the tone early on in this relationship is very important. If you act haphazardly or give off the impression of disorganization it could impair the relationship you need to survive.

To help you implement process around your service, we've created the below checklist. You can use this as is but it's advised that you modify it to fit your individual work style. The services you offer and your experience will influence the creation and the ongoing edits of the document. You may also want to consider translating this information into a wiki or similar system for each customer.

LEARN MORE ABOUT THE AT&T CYBERSECURITY MSSP PROGRAM

The AT&T Cybersecurity MSSP partner program is targeted at channel partners who deliver security solutions to the SMB. With its simplicity, reliability and value, AlienVault® Unified Security Management® (USM) software is well positioned to be the technology of choice for many security services.

Why AT&T Cybersecurity?

- Easy centralized management with federated features
- Fully supported software based on open source security tools
- Cutting edge, crowd-sourced security intelligence from AT&T Alien Labs® and Alien Labs® Open Threat Exchange® (OTX™)
- Easily build security offerings around AlienVault USM to provide SIEM, Network IDS, Host IDS, File Integrity Monitoring, Vulnerability Assessment and more.
- Flexible deployment options: cloud, hybrid and on-premises
- Full suite of compliance reporting
- "Pay as you Grow" licensing mode

To learn more about becoming an AT&T Cybersecurity MSSP, send an e-mail to partners@alienvault.com.

MSSP CHECKLIST

Network information

External network ranges

Internal network ranges

VLANS / defined zones

Remote sites

DNS servers

NTP servers

LOGGING DEVICES

Devices which will emit logs for processing

Hostname	IP address	Type	Vendor	OS / version

CONTACT INFORMATION

Name	Contact hours	Phone	Email

PRIORITY ESCALATION CONTACTS

SCHEDULED EVENTS

Describe any change control procedures, schedules, times when there should be no outage or change freeze periods.

Vulnerability scanning – list exclusions or ranges to be scanned and permitted frequency

Active asset discovery - list exclusions or ranges to be scanned and permitted frequency

Endpoint protection – list current software or servers for OSSEC installation

Network intrusion – list possible devices for gathering network data. e.g. SPAN/RSPAN/TAP

Netflow – list devices sending Netflow data

Acceptable or non-permitted applications e.g. Skype, Facebook, BitTorrent