The Power of Integration

Getting Maximum Value Out of Your Next Security Tool Project

Brian Read
Security Practice Manager
Conexsys Communications Ltd.
Who is Conexsys Communications?

- Security service provider and integrator
- 55 years in the Canadian IT market
- Trusted advisor to many large customers in the financial, energy and government sectors
- Specialize in multi-vendor environments

Acquired by Optiv Security
Who is Conexsys Communications?

- Security service provider and integrator
- 55 years in the Canadian IT Market
- Trusted advisor to many large customers in the financial, energy and government sectors.
- Specialize in multi-vendor environments
Who am I?

- Security Practice Manager at Conexsys Communications Ltd.
- SME for PIDM, Vulnerability Management Solutions
- Advise clients on controls design and other strategic security projects
- Help clients with project requirements and product selection
Today’s Goals

• Categorize 3 most common ways vendors integrate their security products
• Outline the lessons I’ve learned from integrating Conexsys’ partner products
• Give you 5 “insider tips” for how to approach integration in your next RFP or vendor product discussion
Why Integrate Security Products?

- Share information:
  - Endpoint agent acting on information from our threat feeds.

- Leverage each others features:
  - NAC system that can quarantine via the firewall

- Address a missing feature:
  - Third party 2FA, Third party Encryption...
Why Integrate Security Products?

- Share information:
  - Endpoint agent acting on information from our threat feeds.

- Leverage each others features:
  - NAC system that can quarantine via the firewall.

- Address a missing feature:
  - Third party 2FA, Third party encryption.

Decrease Risk

Lower Costs
1. Out of the box integration
2. Grow your own integration
3. Third party orchestration
“Selected endpoint agent must integrate with our existing {FireEye, Tenable, A10, AWS, Ixia, Active Directory...}.”
Vendor Response: We Work With Almost Everyone!

THREAT INTELLIGENCE
- sentrybay
- NetClean
- BlueLiv
- SenseCy
- IID
- mnemonics
- PHISHLABS
- Zerofox
- sentrybay

MOBILITY
- Communitake
- MobileIron
- Acronis
- FancyFon
- SAP
- Skycure
- Maas360
- airwatch
- Sophos

CLOUD
- vmware
- openstack
- Amazon Web Services
- ADVA
- Microsoft Azure

101 TECHNOLOGY PARTNERS

ENFORCEMENT
- SECURE
- Bit9
- Tripwire
- FEITIAN
- AVANAN
- Viewfinity
- RSA
- CloudLock
- Zscaler

MANAGEMENT
- RedSeal
- Splunk
- Trustwave
- RSA
- GreenID
- Lookout
- F5
- Invincea

INFRASTRUCTURE
- Alcatel-Lucent
- Avaya
- Radware
- Avaya
- ECI
- Intel
- Telco Systems
- Riverbed
- Siemens
- Microsoft

SECCTOR

t Security Education Conference

CONEXSYS
Communications Limited
“Selected firewall must support the following protocols {802.1x, SAML, LDAP, ...}.”
Vendor Response: Yes We Love and Support Standards!

**Authentication Methods:**
- Username and Password, LDAP, Windows authentication, RSA SecurID, Web SSO, RADIUS, PKI and smart cards

<table>
<thead>
<tr>
<th>Integration</th>
<th>SaaS federation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SSO integration with enterprise and cloud services</td>
</tr>
<tr>
<td></td>
<td>Connect to, query and retrieve data from enterprise resources such as DBMSs and Microsoft* SharePoint*</td>
</tr>
<tr>
<td></td>
<td>SAML integration</td>
</tr>
<tr>
<td></td>
<td>Amazon AWS AMI integration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SOA</th>
<th>Simple Orchestration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WS-* support</td>
</tr>
<tr>
<td></td>
<td>XACML</td>
</tr>
<tr>
<td></td>
<td>MOM mediation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Auth &amp; Comms</th>
<th>WebSocket</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XMPP</td>
</tr>
<tr>
<td></td>
<td>OAuth and OpenID Connect</td>
</tr>
</tbody>
</table>
So Product A Has Out of the Box Support for Product B

- Check that box
- What could go wrong...
- Not all the features you want are "integrated"
- Integration is in the wrong "direction"
- Supported on the latest/older versions only
- Some product reconfiguration may be required
- Define exactly what integration you want to achieve as specifically as possible – early in the project.
The Devil is in the Details

- What specific features are integrated?
- What “direction” is the integration?
- What versions of the products are integrated?
- What modifications must be made to each product?
VM product must support threat feeds from leading vendors

VM product must act on threat information from threat feeds using STIX or JSON

VM product must adjust vulnerability status based threat intel from FireEye iSIGHT
Insider Tip #2 – Ask for Proof

- Detailed case study demonstrating the 2 products integrating
- Detailed configuration documentation showing how the integration works
DESCRIPTION OF PRODUCT INTEGRATION

The joint CyberArk and SailPoint solution is bi-directional, whereby user provisioning to CyberArk is performed directly from SailPoint based on active directory groups, policies and an approval process defined within SailPoint. In addition, CyberArk collects privileged user data, account information and access data and sends it to SailPoint.

By centralizing and unifying identity and access governance of privileged and non-privileged users, organizations can:

- Fully manage privileged user (individuals/applications) lifecycles:
  - Create, review and approve privileged user access permissions based on group affiliations, roles and other commonalities directly from IdentityIQ. All privileged access requests are verified using an automated approval workflow. Once approved, data is automatically synchronized with the CyberArk Privileged Account Security Solution and a privileged user is added to the relevant privileged account(s).
  - Update user/group access privileges directly from IdentityIQ to avoid orphan privileged accounts, privileged entitlement creep, and excess privileged permissions. Updated access
INSTALLATION STEPS

On the server for the CyberArk – SailPoint integration:

1. Install PACLI (refer to CyberArk’s “Command Line Interface Guide and Reference”); Set PACLI in your PATH environment variable.
3. Install AIM (Refer to CyberArk’s “Credential Provider and ASCP Implementation Guide”). AIM (Application Identity Management) is required for the CyberArk integration package to retrieve the credential for the STI MySQL Database.
4. Define the Application “CyberArk-SailPoint” within CyberArk
5. Configure the application to have access to the STI Staging Database
6. Load the CyberArk-STI Configuration xml file into SailPoint IdentityIQ (contained in the integration package downloaded from Compass)
7. Configure CyberArk-SailPoint Integration:
   a. Extract CyberArk-SailPoint.zip
   b. Update Vault.ini to point to the Vault to be used for the integration
   c. Create CyberArk User for extracting data from the CyberArk Vault, and to process provisioning actions to CyberArk Vault using PACLI. This user will need the following:
      i. All Vault Authorizations (to be able to grant permissions, this user will need to have them):
         ▪ Add Safes,
         ▪ Audit Users,
         ▪ Add/Update Users,
         ▪ Reset Users’ Passwords,
         ▪ Activate Users,
         ▪ Add Network Areas,
         ▪ Manage Directory Mapping,
         ▪ Manage Server File Categories,
         ▪ Backup All Safes,
         ▪ Restore All Safes
      ii. Member of Auditors Group (to have audit permissions on all the safes in the Vault)
      iii. All permissions on Safes that will be part of the Entitlement set of permissions that the provisioning actions will be granting or revoking. It could be member of a group that grants all the needed permissions on safes.
   d. Create credential file for the user created in previous step. Refer to “Appendix A: Creating Credential Files” of the “Privileged Account Security Installation Guide” from CyberArk’s Documentation set.
Insider Tip #2 – Ask for Proof

- Detailed case study of the 2 products integrating
- Detailed configuration documentation
- Proof of concept
  - Product Vendor or Integrator lab
  - (or POC your own lab...)

SECITOR

Security Education Conference

CONEXSYS

COMMUNICATIONS LIMITED
3 Ways Products Can Integrate

1. Out of the box integration
2. Grow your own integration
3. Third party orchestration
Unique Requirement:

- customizable reporting
- custom alerting
- support less common product

“Load balancer must support dynamic additions of new servers based on our ServiceNow ticket”
Vendor Response: We Support That...Through Our API!

*aXAPI Custom Management*

The Thunder Series and AX Series Application Delivery Controllers (ADCs) feature aXAPI, a REST-based Application Programming Interface (API), enabling remote interaction from third-party applications. See https://www.axapi.com/ for more information.

You can write a script that adds a server to the load balancer.
Insider Tip #1 Revisited: Fully Define Your Requirements

- Make sure the API supports the functionality you are looking for
- You may be surprised with what’s missing in a v1.0 or v2.0 API
- Review the API documentation
- Simple script vs complex coding effort
- Remember the SDLC:
  - Build
  - Test (security, performance, function)
  - Deploy and redeploy
  - Repeat
- What level of support is required?
- Is there a development community to draw from?
A10 Script already exists on GitHub
The product vendor or integrator can likely write the integration
– and test
– and troubleshoot
– and support
They may already have it written
Insider Tip #4: Investigate Outsourcing

- Negotiate some custom integration as part of the project purchase
3 Ways Products Can Integrate

1. Out of the box integration
2. Grow your own integration
3. Third party orchestration
“Selected firewall must support existing workflow of:”

– Realtime firewall log review and automatically extract critical alerts
– Open a ticket with source and other and key info
– Connect to perimeter device and shun IP address
– Email SOC manager
Firewall Vendor Response: Ummmm...
Insider Tip #5: Explore SOC Orchestration Tools

• Automate your playbook
Insider Tip #5: Explore SOC Orchestration Tools
Insider Tip #5: Explore SOC Orchestration Tools

- Automate your playbook
- Free analysts from level 1 tasks and reallocate them to more productive tasks
In Summary

1. Fully define the integration
2. Ask for proof
3. Evaluate the level of effort of any custom integration work
4. Don’t rule out outsourcing
5. See if third party orchestration tools can solve the problem
Follow Conexsys on Twitter: @conexsyscomm

For any pdf of this presentation or any technical questions come by the Conexsys booth or contact me at brianr@conexsys.net

Drop off a card at the booth and win a $100 Tims Card