“UCR’s implementation of a security dashboard (nominally designated SecTools) is a wonderfully flexible and useful framework for viewing current security incidents and for gaining an understanding of the current security posture on campus. Currently the information provided in the dashboard includes the number and IPs of external hosts that have null routes in place, a listing of current security events such as ssh brute force attacks, and global information about attacking hosts. Each of the above can be focused on so that low level details are revealed. Thus, not only does the SecTools site provide a window into current security events and preventions, it allows operational personnel to turn off campus systems, whitelist others, and, in the future, look at campus servers for adherence to campus security standards. The security tools platform is a great advancement in UCR’s security infrastructure.”

Russ Harvey, Director, Computing Infrastructure & Security, Computing & Communications

Campus Impact

The growth of the UCR campus in recent years has forced UCR Computing and Communications to reconsider how IT resources are provisioned, monitored, and protected. With hundreds of systems hosting applications and providing critical services for campus needs, it has become clear that protecting these systems and obtaining enterprise visibility into the active security environment can be a
complicated and expensive challenge. Moreover, IT security teams can quickly become overloaded with data and manual processes can significantly hamper the ability to rapidly respond to evolving threats. As campus services have grown and security threats continuously evolve, UCR wanted to develop a better way to understand and manage its enterprise security environment.

**Business Need**

A proposal was laid out to significantly improve UCR’s enterprise security capabilities by building a new security ecosystem utilizing free open-source software (FOSS) and inexpensive commodity hardware solutions. A central component of this security ecosystem would be a Security Information and Event Management system (SIEM) that would aggregate large amounts of data and correlate security events across a multitude of systems and network devices. Vendor SIEM solutions can be expensive, difficult to customize and have limited flexibility for dynamic environments operating with limited resources. The challenge was to build a system that leveraged FOSS as much as possible and fill in the gaps with custom software that provided SIEM capability without significant investments in additional infrastructure or personnel.

To meet these challenges, UCR has successfully created and deployed a core component of our new ecosystem called Security Tools or simply, SecTools. SecTools provides a real-time dashboard displaying host and network security alerts using data acquired from intrusion detection sensors. Various incident response tools have been added to assist security teams in quickly responding to events. Additionally, SecTools automatically responds to certain events by blocking the attacker’s access to campus resources without requiring manual intervention by IT security staff. Ultimately, SecTools will acquire security relevant data from many sources including directory services and inventory management systems to help enhance incident response activities.
Highlights
The SecTools dashboard provides an enhanced situational awareness capability that UCR did not have before. SecTools provides a single, unified environment for viewing and responding to security events based on data acquired from host intrusion detection (HIDS) and network intrusion detection systems (NIDS). Security events are categorized and reported based on defined levels of severity. Security personnel can view the specific log or audit records from a particular host or device that triggered the respective security event.

Existing legacy incident response tools have been updated, optimized and integrated into the SecTools environment. Security staff have the ability to block active attacks (internal or external) via campus border routers through simple interfaces. Event data is correlated from intrusion detection sensors giving staff insight into the behavior of a particular attack before making a response decision.
Technology and Implementation

Free and Open Source Technologies
There have been no software or licensing costs to implement SecTools. The SecTools dashboard and HIDS interface layer were built using Mojolicious, a real-time web services framework, in conjunction with a MySQL database backend. Host and network intrusion detection capability for event collection and correlation use the open source solutions OSSEC and Bro-IDS. Both systems have a robust rules framework allowing new rules to be quickly implemented to deal with evolving security vulnerabilities.

Web Services Architecture
SecTools has been implemented using a REST web services framework utilizing simple HTTP GET or POST operations. This provides an easy to use API for storing and retrieving security event data while making it easy to add new functionality for future tools and leverage new sources of event data. SecTools also provides wrapper services for network devices or systems such as Cisco LAN Management Solution, providing a convenient way for security staff and their applications/scripts to retrieve data without needing to deal with the complexities of the vendor API. The web services offer data in HTML, JSON or XML formats.

Dashboard Capability
Security engineers are provided a unified dashboard allowing an integrated visibility into the security environment. Additionally, various security tools have been integrated into the environment providing a single point for security event management and incident response.

Intrusion Prevention
In order to implement SecTools, it was critical for the Security team to work with the Network Services Group. Personnel in both Security and Network Services cooperated to implement a hardware and software solution allowing SecTools to automatically respond to security threats by blocking malicious actors at campus border routers. Capability is also in place to quickly respond to internal campus incidents.
Cross-Platform Analysis
OSSEC HIDS provide cross-platform data collection, file integrity monitoring and log analysis for Linux, Unix (Solaris, AIX, HP-UX, BSD), Mac and Windows platforms. Agentless monitoring is also available for monitoring special purpose appliances or network devices (e.g. network switches). OSSEC also supports a large collection of host services including web servers, mail servers, directory services, databases and firewalls. A web services wrapper for OSSEC was written to facilitate data exchange with SecTools.

Collaborative Response
The handling of IT security incidents are occasionally complicated by the division of responsibilities in the UCR environment. Security staff may act on given activity behind the scenes, while support staff deal with the clients directly. SecTools optimizes the response security staff have to incidents, but it also provides support personnel capabilities to continue the remediation process of incidents without requiring security staff intervention.

Case Studies

Campus E-Mail System
As with many universities, phishing attacks are a persistent and evolving problem at UCR. Phishers are constantly changing their tactics with hundreds of targeted phishing sites being setup daily. The challenge was to implement a system that could monitor this behavior and allow for quick updates to evolving threats. SecTools and OSSEC were chosen to provide an external security monitoring service to correlate events for detecting suspicious mail traffic, phished accounts and automatically generating security reports. SecTools provided automated response to security threats such as SMTP brute force attacks and account harvesting by blocking malicious users via campus border routers. This system has provided a real-time assessment and response mechanism for UCR mail systems processing millions of messages each day. In the last couple months, over 60 compromised (phished) accounts have been successfully identified and remediated. Additionally, over 1500 mail server attacks have been stopped.

Host Intrusion Detection/Prevention
UCR is in the process of deploying HIDS and NIDS sensors to a wide range of critical systems. OSSEC sensors are currently monitoring various types of systems and service daemons. Certain types of attacks are reported to SecTools for automatic response, which includes blocking the attacks at campus border routers and alerting administrators of these actions. To date, over 300 attacks against UCR systems have been stopped primarily through automated intrusion prevention. These automated responses have helped offload routine remediation tasks from security teams.

Compliance
UCR has to meet compliance objectives like any other large organization. Specifically, we have systems that must meet PCI DSS compliance. SecTools and OSSEC were chosen to provide monitoring and analysis services to meet specific security control objectives outlines in PCI DSS, such as:

- File Integrity Monitoring
- Log collection, analysis and reporting
- Intrusion detection and prevention
The system will also help meet specific control objectives of IS3 compliance. Administrators can be alerted regarding file integrity violations and utilize SecTools to view the specifics of the violation. Corrective action can then be immediately taken. Future phases of this project will provide scheduled and on-demand compliance assessments, which will immediately report noncompliance to SecTools via its web service interface.

**Cross-Functional Team Coordination**
UCR Computing Support (Help Desk) personnel have the ability to release security blocks for internal UCR hosts that were previously infected or otherwise compromised. SecTools has provided basic authorization features giving Help Desk staff a modified dashboard and applications to assist in responding to trouble tickets and perform basic user/host remediation tasks. For example, Help Desk personnel are able to work directly with students to release network blocks put in place due to malware infected machines or DMCA violations.

**Testimonials**

"A single place to go for security events and remediation information has long been a goal for our organization. Because it is architected and implemented using open source, standards based tools, the SecTools framework can meet our immediate needs and be extended to encompass future aspects of our security ecosystem. SecTools is our Killer App for security management."

--- Bob Grant, Interim Executive Director, Computing & Communications

**Timeline**

September 2012       Project Initiation  
November 2012        System Testing with C&C  
December 2012        Phase I Deployment (Dashboard, HIDS Module)  
May 2013             Phase II Deployment (HIDS Agents)  
August 2013          Phase III Deployment (NIDS)  

**On the Web**

Production site: https://sectools.ucr.edu

**Team Members**

<table>
<thead>
<tr>
<th>Computing &amp; Communications</th>
<th>Dept., Org., Partners, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stephen Hock</td>
<td>Computing &amp; Communications</td>
</tr>
<tr>
<td>Nicholas Turley</td>
<td>Computing &amp; Communications</td>
</tr>
<tr>
<td>Michael Brandeis</td>
<td>Computing &amp; Communications</td>
</tr>
<tr>
<td>Jonathan Ocab</td>
<td>Computing &amp; Communications</td>
</tr>
</tbody>
</table>
Submitted By
Nicholas Turley
Computing Infrastructure Security Analyst
Computing & Communications
University of California, Riverside
nickturley@ucr.edu
(951) 827-3070