ICS Security Monitoring

INFRASTRUCTURE

MINING & METALS

NUCLEAR, SECURITY & ENVIRONMENTAL

OIL, GAS & CHEMICALS

Moses Schwartz
Security Engineer
Computer Incident Response Team
Bechtel Corporation

State of the Field

- **Enterprise IT Security**
  - Emphasis on **active defense**, defense-in-depth, iterative improvement.
  - Continuous monitoring by dedicated teams.
  - Vulnerability management program and regular patching.
  - Centralized logging and alerting.
  - Proactive “hunting” informed by threat intelligence.
  - Attacks are identified early and remediated quickly.
- **Industrial Control Systems (ICS) Security**
  - Emphasis on passive protection (firewalls, antivirus).
  - No patches, few updates.
  - Attacks are identified by impact on process.
  - Remediation may require plant shutdown, extensive re-engineering.

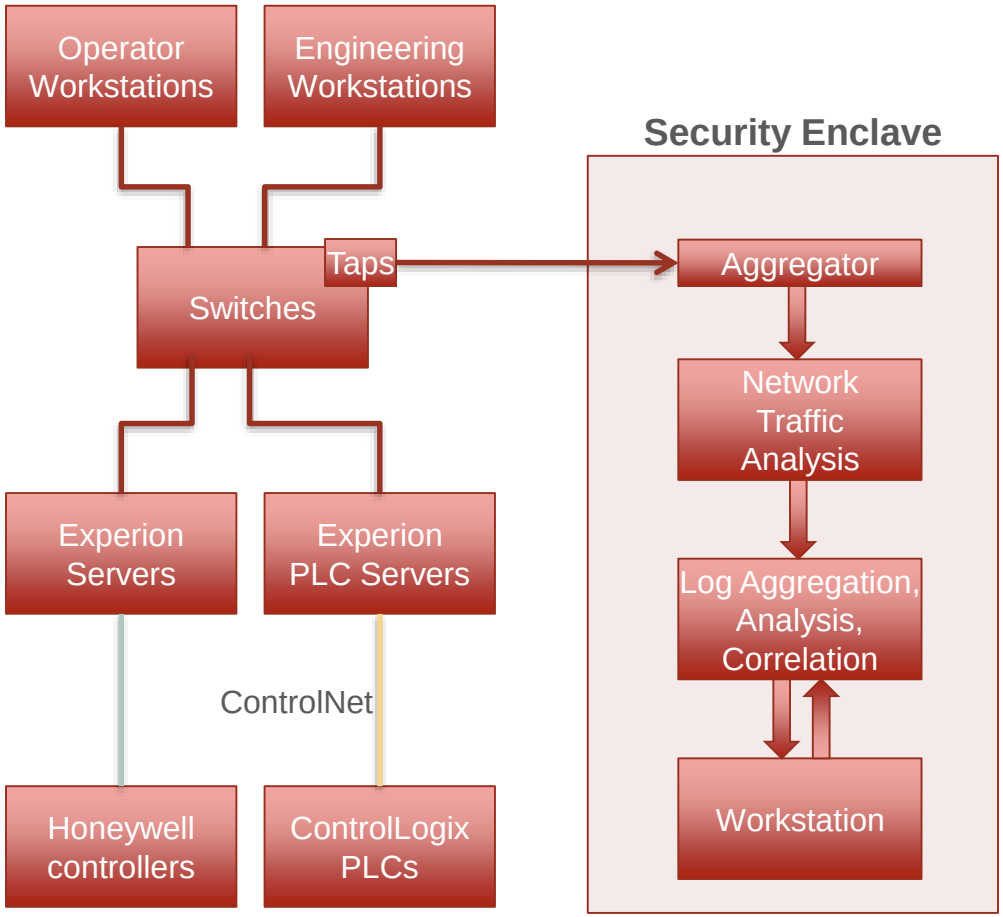
Motivation

- All systems are vulnerable. ICS are particularly weak.
- Attackers have an initial asymmetric advantage.
- Post-exploitation, defenders have the upper hand.
  - The initial foothold is almost never the final target.
  - Attackers are operating in enemy territory.
  - Lateral movement and privilege escalation can be detected.

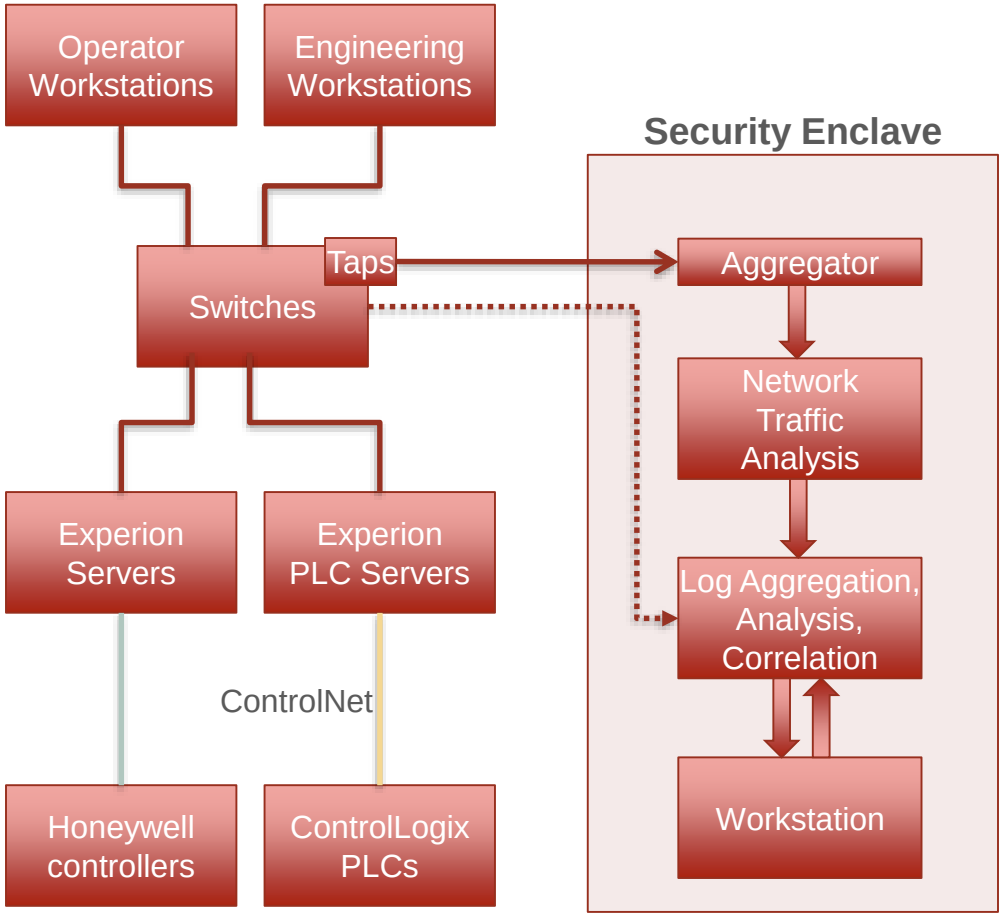
Bringing Modern Tools to ICS Security

- Focus on monitoring and detection.
  - Emphasis on passive and low-impact techniques.
  - Leverage in-house experience with security monitoring.
  - Require human-in-the-loop and encourage active defense.
- Network Security Monitoring (NSM).
  - Deep packet analysis of raw network traffic.
- Security Information and Even Manager (SIEM).
  - Centralized log database.
  - Searching, correlation, alerting.

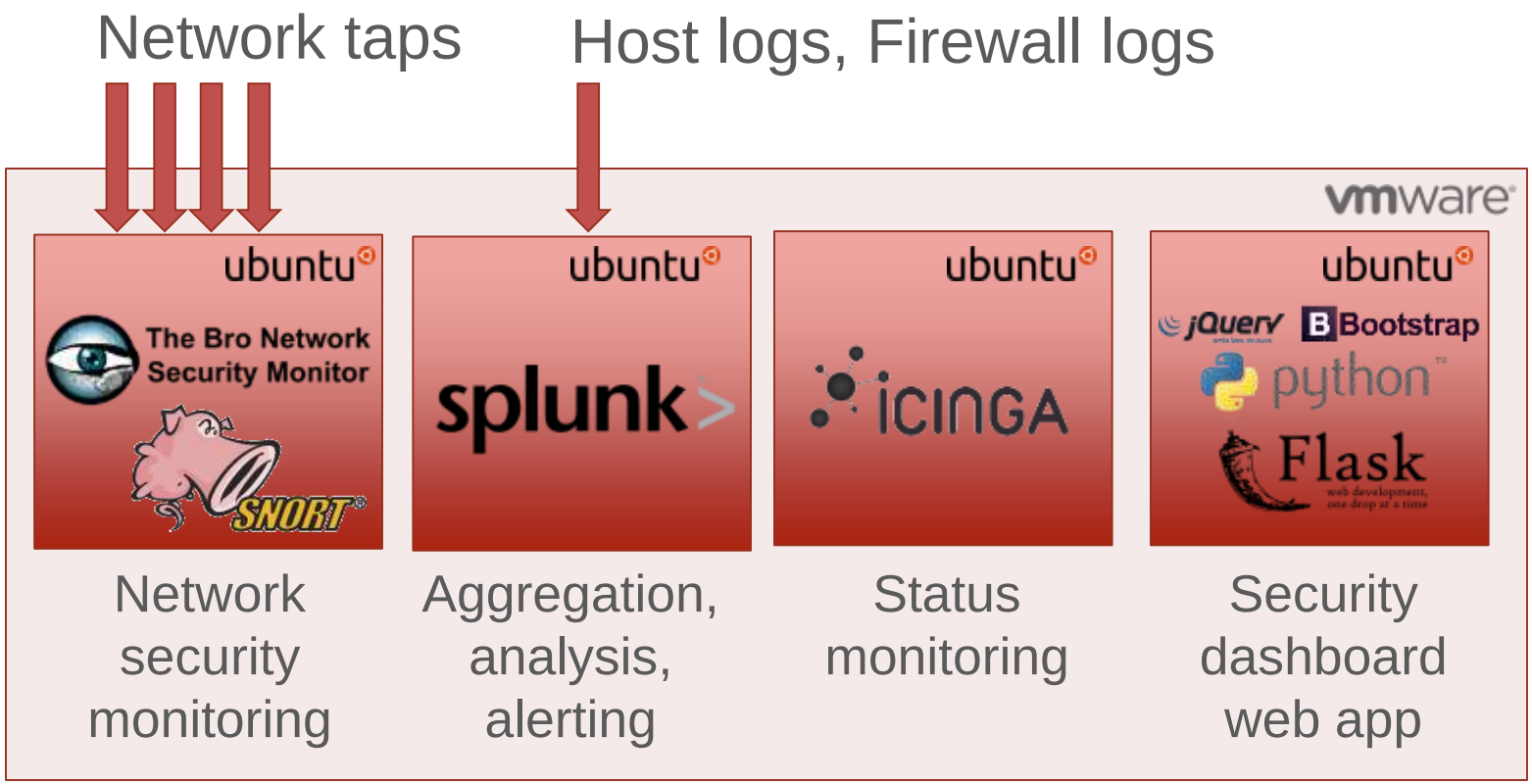
ICS Network Security Monitoring



ICS Network Security Monitoring + Security Information Event Manager

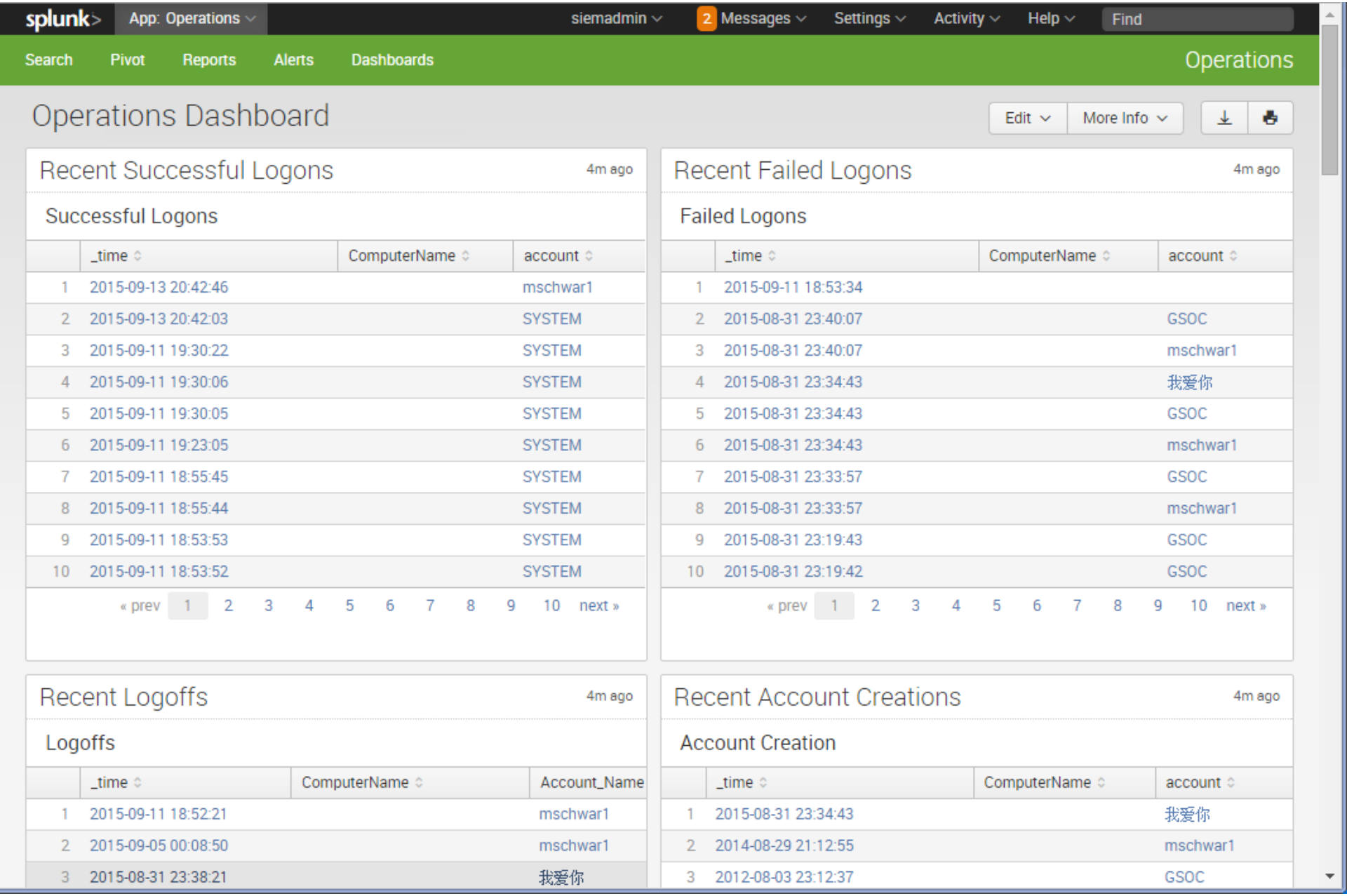


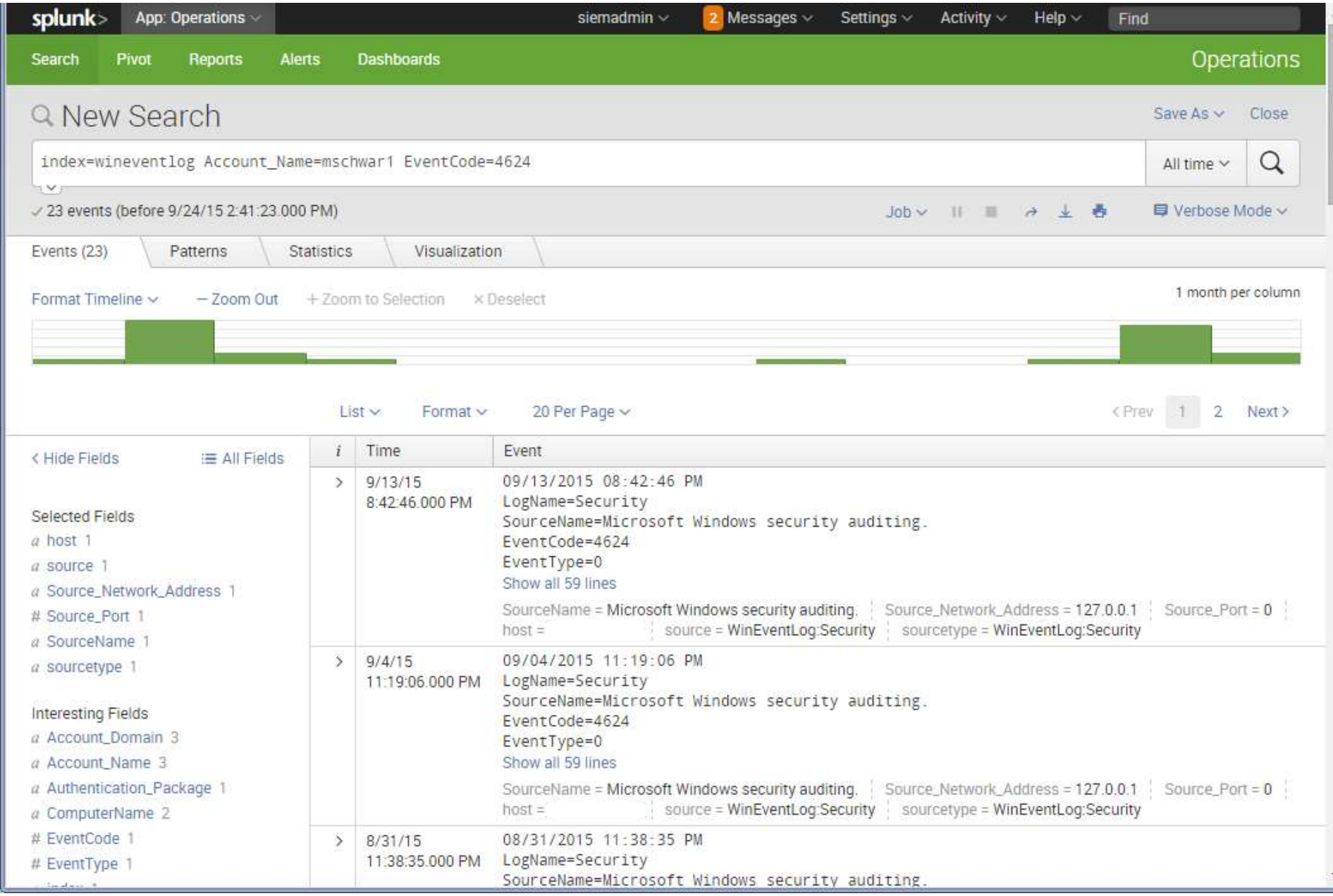
NSM / SIEM infrastructure (v1)

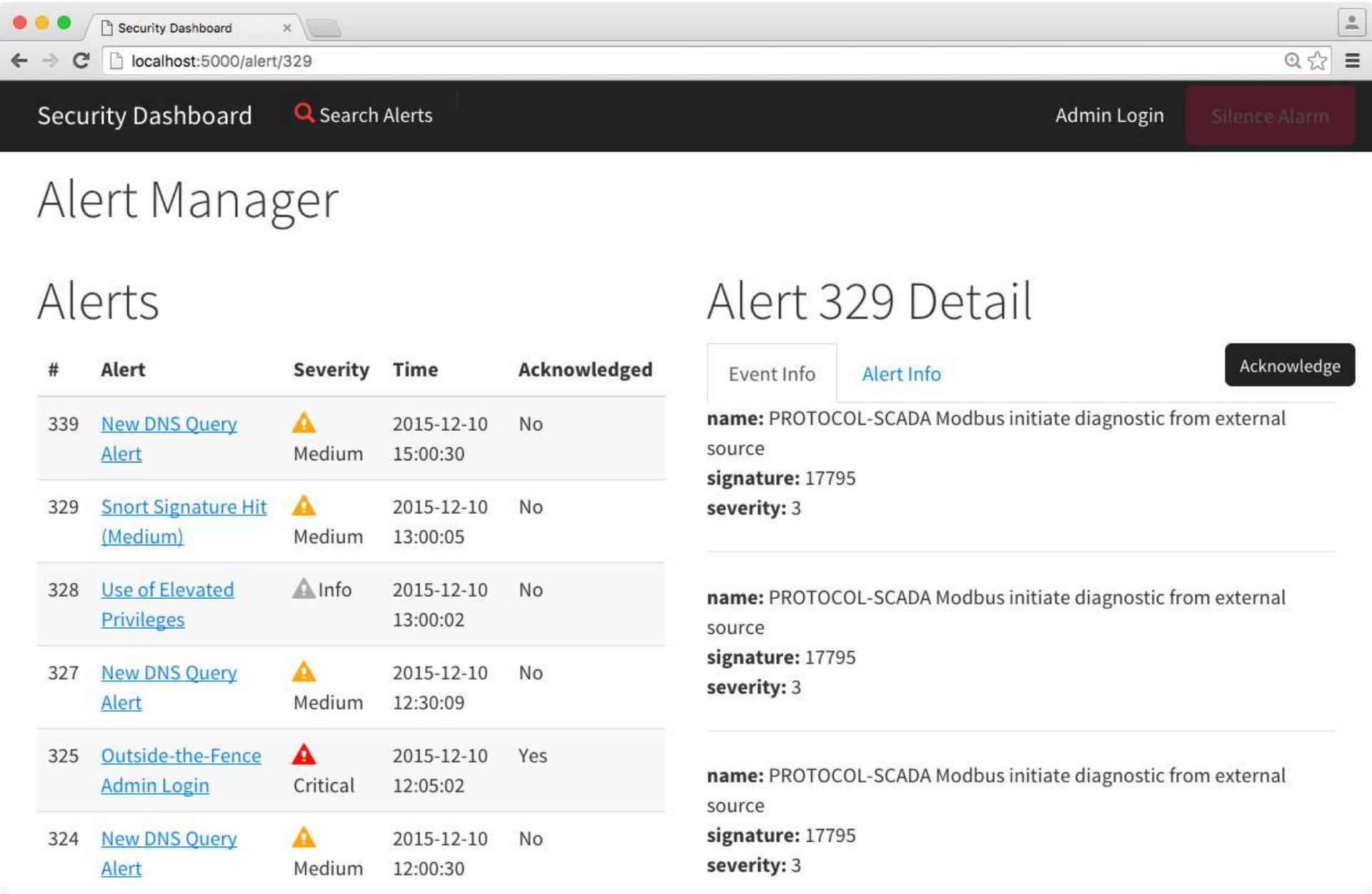


System Interaction: Dashboards

- Splunk Dashboards.
  - System overview.
  - Auditing.
  - Troubleshooting.
  - General network situational awareness.
- Security Dashboard.
  - Light-weight ticketing system.
  - Displays alerts.
  - Plays audible alarms.
  - Enforces human-in-the-loop workflow.


splunk>
App: Operations
siemadmin
2 Messages
Settings
Activity
Help
Find
Search
Pivot
Reports
Alerts
Dashboards
Operations
Operations Dashboard
Edit
More Info
Recent Successful Logons
4m ago
Successful Logons
_time
ComputerName
account
1 2015-09-13 20:42:46 mschwar1
2 2015-09-13 20:42:03 SYSTEM
3 2015-09-11 19:30:22 SYSTEM
4 2015-09-11 19:30:06 SYSTEM
5 2015-09-11 19:30:05 SYSTEM
6 2015-09-11 19:23:05 SYSTEM
7 2015-09-11 18:55:45 SYSTEM
8 2015-09-11 18:55:44 SYSTEM
9 2015-09-11 18:53:53 SYSTEM
10 2015-09-11 18:53:52 SYSTEM
« prev 1 2 3 4 5 6 7 8 9 10 next »
Recent Failed Logons
4m ago
Failed Logons
_time
ComputerName
account
1 2015-09-11 18:53:34
2 2015-08-31 23:40:07 GSOC
3 2015-08-31 23:40:07 mschwar1
4 2015-08-31 23:34:43 我爱你
5 2015-08-31 23:34:43 GSOC
6 2015-08-31 23:34:43 mschwar1
7 2015-08-31 23:33:57 GSOC
8 2015-08-31 23:33:57 mschwar1
9 2015-08-31 23:19:43 GSOC
10 2015-08-31 23:19:42 GSOC
« prev 1 2 3 4 5 6 7 8 9 10 next »
Recent Logoffs
4m ago
Logoffs
_time
ComputerName
Account_Name
1 2015-09-11 18:52:21 mschwar1
2 2015-09-05 00:08:50 mschwar1
3 2015-08-31 23:38:21 我爱你
Recent Account Creations
4m ago
Account Creation
_time
ComputerName
account
1 2015-08-31 23:34:43 我爱你
2 2014-08-29 21:12:55 mschwar1
3 2012-08-03 23:12:37 GSOC


splunk> App: Operations siemadmin 2 Messages Settings Activity Help Find
Search Pivot Reports Alerts Dashboards Operations
New Search
Save As Close
index=wineventlog Account_Name=mschwar1 EventCode=4624
All time
23 events (before 9/24/15 2:41:23.000 PM)
Job Verbose Mode
Events (23) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect
1 month per column
List Format 20 Per Page
Prev 1 2 Next
Hide Fields All Fields
Selected Fields
a host 1
a source 1
a Source_Network_Address 1
Source_Port 1
a SourceName 1
a sourcetype 1
Interesting Fields
a Account_Domain 3
a Account_Name 3
a Authentication_Package 1
a ComputerName 2
EventCode 1
EventType 1
i Time Event
9/13/15 8:42:46.000 PM
09/13/2015 08:42:46 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4624
EventType=0
Show all 59 lines
SourceName = Microsoft Windows security auditing. Source_Network_Address = 127.0.0.1 Source_Port = 0
host = source = WinEventLog:Security sourcetype = WinEventLog:Security
9/4/15 11:19:06.000 PM
09/04/2015 11:19:06 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4624
EventType=0
Show all 59 lines
SourceName = Microsoft Windows security auditing. Source_Network_Address = 127.0.0.1 Source_Port = 0
host = source = WinEventLog:Security sourcetype = WinEventLog:Security
8/31/15 11:38:35.000 PM
08/31/2015 11:38:35 PM
LogName=Security
SourceName=Microsoft Windows security auditing.



Alert Examples

Audit Network/Host Changes
- New Account Created
- New Account Login
- New DNS Query
- New Windows service installed
- New Source/Destination IP
- New Source/Destination Connection
- New MAC Address

Monitor System Health
- High Disk Usage
- Splunk Internal Errors

Detect Targeted Events
- Snort Signature Hit
- PowerShell Launched
- Outside-the-Fence Login
- Login on Many Hosts
- Many Failed Logins
- Login Success After Many Failures

Auditing and Compliance
- Use of Elevated Privileges
- USB Device Connected
- User Login/Logoff
- System Restart/Shutdown

System Summary

- Baseline system.
  - Applies modern IT security tools to ICS networks.
  - Provides basic visibility into ICS network and hosts.
  - Similar to commercial solutions.
- Enforces a human-in-the-loop and active defense.
- Gives us a starting point to pursue ICS security research with real, rich data sources.

Red Team Detection and Response

- Detection.
  - Laptops re-used between assessments.
  - Post-exploitation toolkit detectable by PowerShell executions.
- Response.
  - Live remote memory analysis.
  - Onsite IT and helpdesk to disable network ports, obtain and image systems, interface with site security.
  - Rootkit-style security agent to maintain control.

Approach

- Log everything, and actually read those logs. Make analysis easy.
- Look for low-level system behavior that is common to attacker toolkits. Infection vectors change, but post-exploitation escalation and lateral movement is constant.
- Never let someone break in the same way twice. Learn from our attackers. Continually develop new alerts.
- Encourage proactive hunting. Practice being the adversary. Test our defenses.
- Fully understand a compromise before acting. When ready to remediate, act quickly and decisively.

Future Work

- Develop better alerts and dashboards.
- Monitor field devices and other ICS components.
- Go deeper than Ethernet: serial, coaxial, RF.
- Explore machine learning techniques for anomaly detection.
- Apply software testing best practices to alerting.

ICS Security Monitoring

INFRASTRUCTURE

MINING & METALS

NUCLEAR, SECURITY & ENVIRONMENTAL

OIL, GAS & CHEMICALS

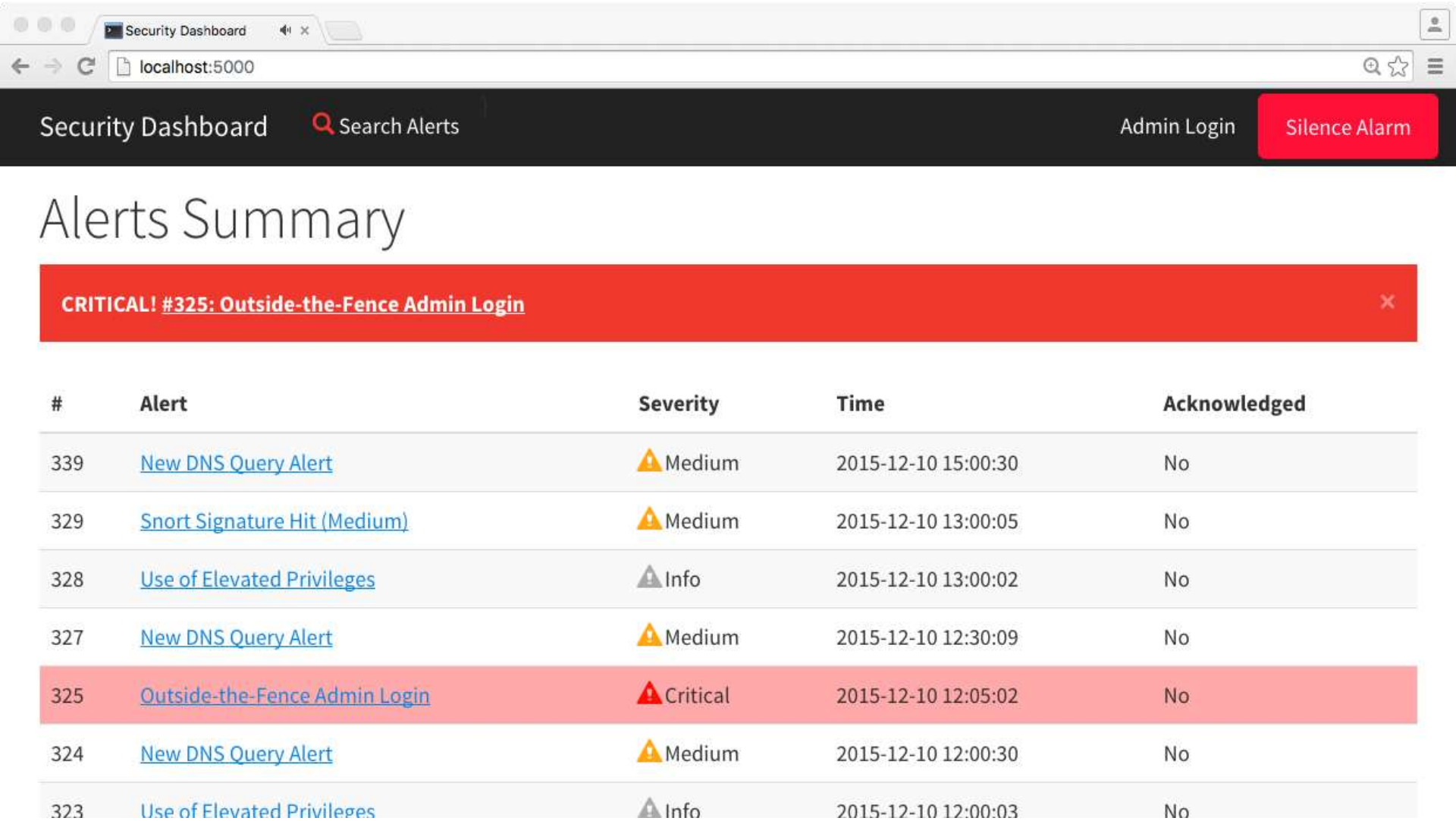
Moses Schwartz
Security Engineer
Computer Incident Response Team
Bechtel Corporation

Case study: Compensating for physical security

- Vulnerability
  - Secondary control room located “outside the fence”
  - Not manned 24x7

- Mitigation
  - Audible alarm for admin logins on outside-the-fence systems

Audible alarms



Case study: PowerShell activity alert

- Windows PowerShell.
  - Scripting/automation framework.
  - Very useful for system administration.
  - Frequently used by attackers.
- We've had an great success identifying attacks by alerting on PowerShell execution.