.conf18

splunk>

Attack Surface Reduction: Using Splunk to Spot the Security Flaws in Your Network

John Rubey | Cyber Defense Consultant, Accenture

JOHN RUBEY

Cyber Defense Consultant, Accenture

ACCENTURE SECURITY

UNMATCHED SCOPE AND SCALE: IMAGINE THE POWER

accenturestrategy accentureconsulting accenturedigital accenturetechnology accentureoperations

ACCENTURE SECURITY

20+ YEARS OF EXPERIENCE

350+ pending and issued patents

$1.2B in FY17 revenue

850+ clients spanning **60+** countries

4 Cyber Fusion Centers

8 Delivery Centers

2 Cyber Labs

DOUBLE DIGIT YOY GROWTH

5,500+ EXCEPTIONALLY SKILLED SECURITY PROFESSIONALS

FUELED BY THE ACCENTURE MACHINE

50 CENTERS

75%+ GLOBAL FORTUNE 500

94 OF THE FORTUNE GLOBAL 100

#1 world leader in providing application services (SAP, Oracle Microsoft, Salesforce)

295,000 Accenture Global Delivery Network: professionals, **150+** countries, **45** languages

#1 WORLDWIDE CLOUD PROFESSIONAL SERVICES PROVIDER

Deep expertise in **40+** industries

Agenda

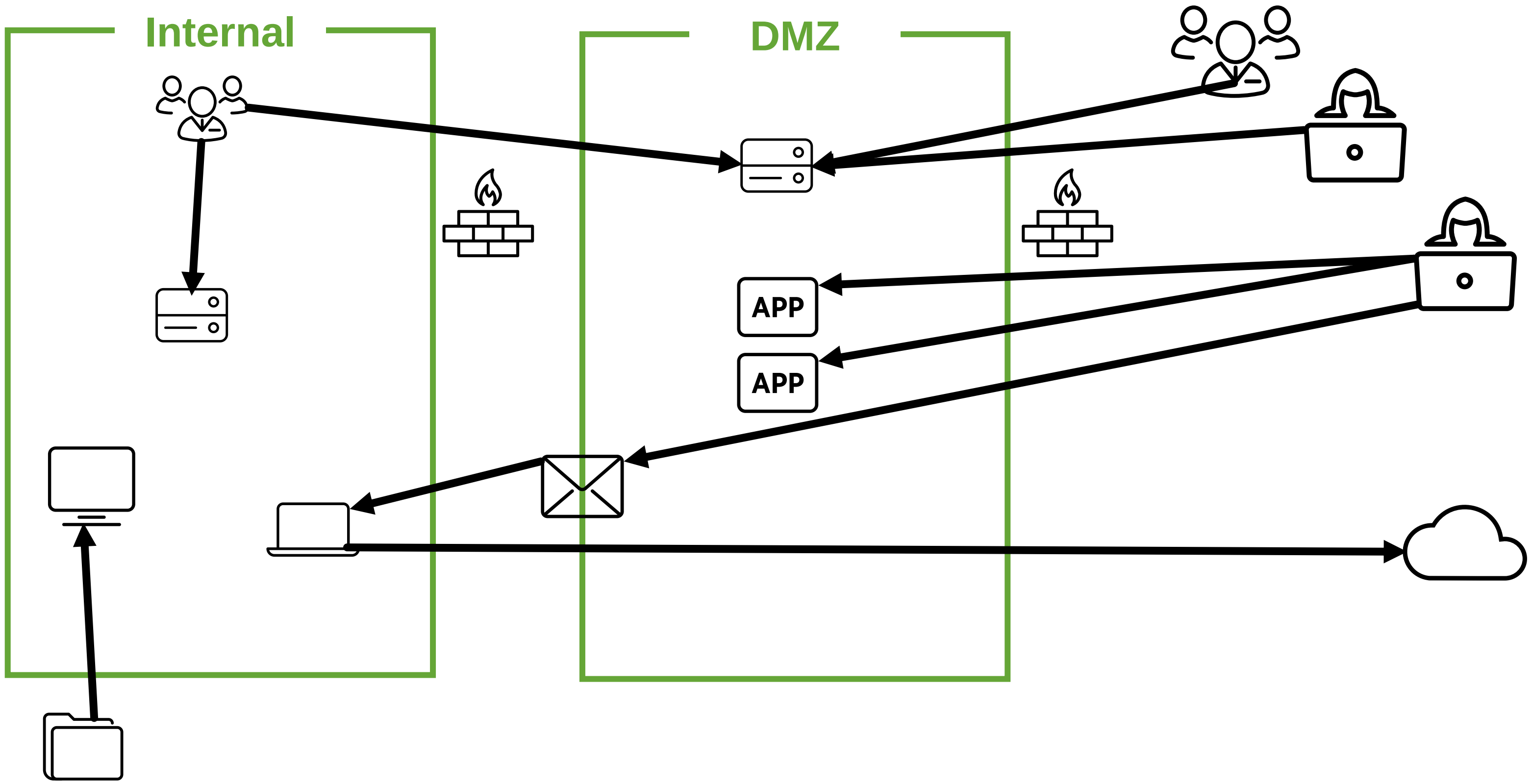
- Introduction to Attack Surface
- Sample Walkthrough
  - Problem Definition
  - Splunk Analysis
  - Remediation Actions

What is the attack surface?

The attack surface describes the company environment’s exposure to attack across multiple vectors

- Numerous vectors exist within the enterprise, including both abuse of legitimate services, misconfigurations, vulnerable services, and others

- **Firewall / Network**
- **Server / OS**
- **Application**
- **Endpoint**
- **User Behavior**
- **More…**



How can we reduce the attack surface?

Continuous maintenance is required to manage the attack surface

Network / Firewall	Remove obsolete firewall rules, increase restrictions on firewall rules, introduce additional IDS/IPS filters, use static firewall rule analysis tools
Server / Operating System	Eliminate insecure configurations, enforce hardening baseline, conduct regular vulnerability scans, monitor server configuration drift
Endpoint	Increase endpoint protection coverage, prevent USB device connectivity
Application	Perform static code analysis, conduct regular application penetration tests, use automated code scanning tools

Challenge

Critical business processes may rely on insecure configurations, so insecure configurations must be eliminated gradually to avoid interruption of business activities. The original context for a configuration must be understood before removal, and often times documentation is unavailable

Splunk Data Sources

Existing Splunk data can help understand the impact of changes to reduce the attack surface

Network / Firewall	**Firewall Logs:** identify unused or risky firewall traffic **IDS/IPS Logs:** identify rules allowing potentially malicious behavior
Server / Operating System	**Windows Logs:** ANONYMOUS LOGIN, interactive service account login, personal admin accounts **Linux Logs:** root login over SSH, anonymous FTP transfers
Endpoint	**AV Operations:** identify hosts without AV protection **Host IDS:** identify usage of USB devices in the network
Application	**Firewall Logs:** identify targets of application vulnerability exploits **Application Logs:** identify malicious URI strings

How Splunk Helps

Splunk provides a dynamic capabilities to understand the attack surface and prioritize actions

Contextual Enrichment

Splunk Enterprise Security provides asset and identity context, prioritizing the vulnerabilities which impact the most critical servers and users

Usage-based Prioritization

Splunk enables us to use activity history identify which vulnerabilities and misconfigurations are being used most frequently so they can be prioritized

Identify Legitimate Usage

Splunk enables us to correlate multiple sources to identify legitimate activity, such as which connections through the firewall result in successful server authentication

Continuous Monitoring

Splunk provides continuous insight into insecure processes within the environment, which may be missed between vulnerability scans

Sample Walkthrough

Permissive Firewall Rules

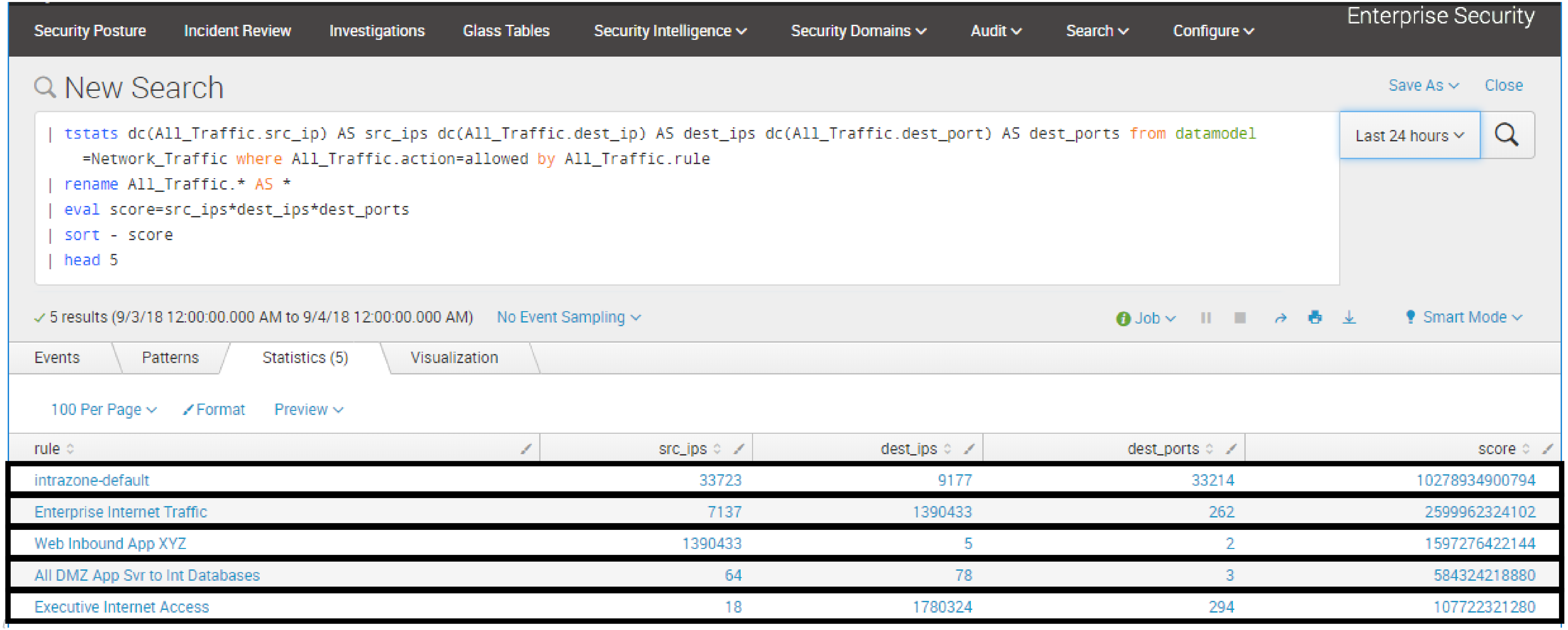
Example Overview: Permissive Firewall Rules

- Firewall rule sets have developed over time in order to provide connectivity between business systems
- Improper firewall rules can allow more traffic than intended through the network, but removing firewall rules can disrupt critical business activities
- Static analysis tools may not help identify the legitimate traffic through an insecure firewall rule
- Iterative approach:
  - Identify a specific firewall rule based on defined criteria, such as most used, externally facing, or other factors
  - Deep dive into the traffic across the rule, and identify the highest traffic patterns
  - Break out rule into individual rules until original rule can be safely removed

Identify a Rule to Focus

Select a specific firewall rule to analyze based on criteria

- For this example, we use a basic query to identify a permissive firewall rule



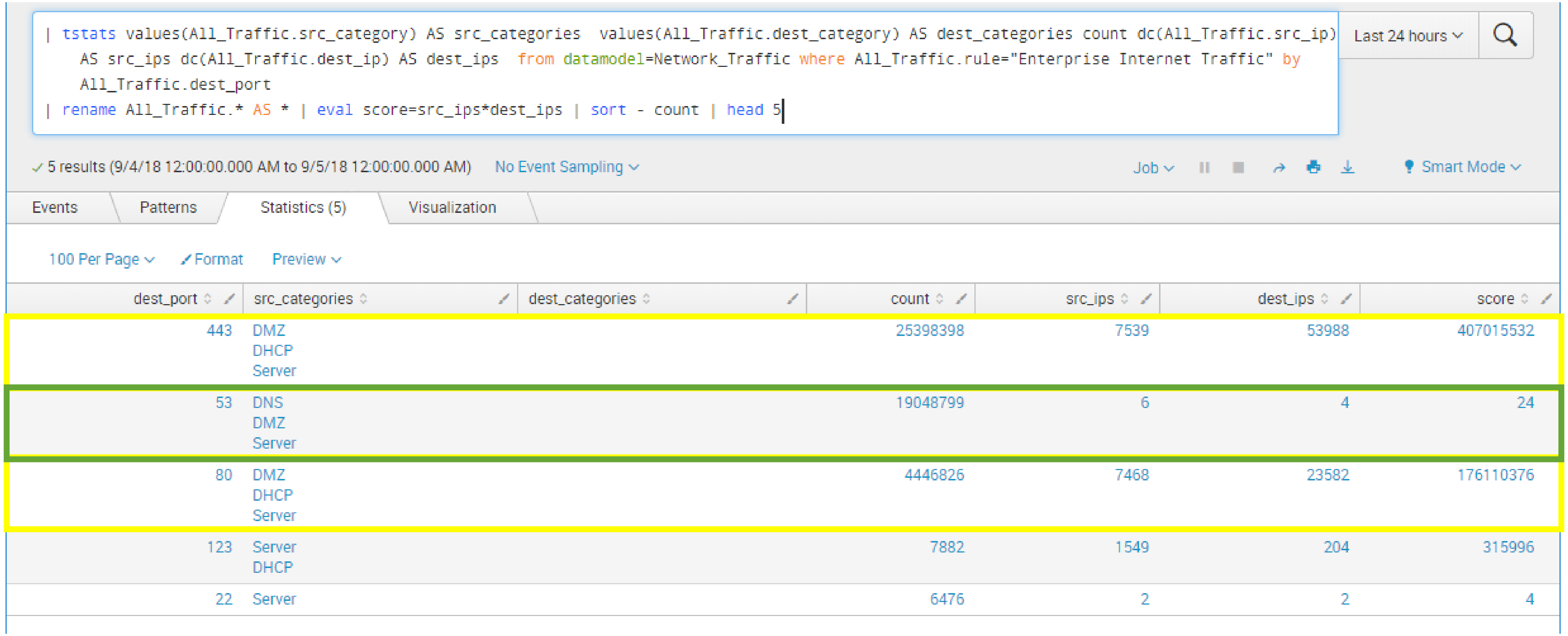
```
| tstats dc(All_Traffic.src_ip) AS src_ips dc(All_Traffic.dest_ip) AS dest_ips dc(All_Traffic.dest_port) AS dest_ports from datamodel
  =Network_Traffic where All_Traffic.action=allowed by All_Traffic.rule
| rename All_Traffic.* AS *
| eval score=src_ips*dest_ips*dest_ports
| sort - score
| head 5
```

✓ 5 results (9/3/18 12:00:00.000 AM to 9/4/18 12:00:00.000 AM)

rule	src_ips	dest_ips	dest_ports	score
intrazone-default	33723	9177	33214	10278934900794
Enterprise Internet Traffic	7137	1390433	262	2599962324102
Web Inbound App XYZ	1390433	5	2	1597276422144
All DMZ App Svr to Int Databases	64	78	3	584324218880
Executive Internet Access	18	1780324	294	107722321280

Drilldown into Traffic for the Rule

Use Splunk to analyze the values of src, dest, and dest_port to identify common patterns



```
| tstats values(All_Traffic.src_category) AS src_categories  values(All_Traffic.dest_category) AS dest_categories count dc(All_Traffic.src_ip)
   AS src_ips dc(All_Traffic.dest_ip) AS dest_ips  from datamodel=Network_Traffic where All_Traffic.rule="Enterprise Internet Traffic" by
   All_Traffic.dest_port
| rename All_Traffic.* AS * | eval score=src_ips*dest_ips | sort - count | head 5
```

✓ 5 results (9/4/18 12:00:00.000 AM to 9/5/18 12:00:00.000 AM) No Event Sampling

dest_port	src_categories	dest_categories	count	src_ips	dest_ips	score
443	DMZ DHCP Server		25398398	7539	53988	407015532
53	DNS DMZ Server		19048799	6	4	24
80	DMZ DHCP Server		4446826	7468	23582	176110376
123	Server DHCP		7882	1549	204	315996
22	Server		6476	2	2	4

ACTION

For this example, create a new firewall rule to specifically cover DNS traffic

Repeat!

Continue to identify "known good" traffic patterns until the remaining rule can be safely removed

- Use the most common traffic patterns to develop new rules, reducing traffic across the permissive rule. Examples of critical traffic to avoid blocking:
  - Active Directory communications
  - Antivirus definitions updates
  - Windows update processes
  - Critical users/critical machines activity
- **Tip:** try including src_category and dest_category to group traffic patterns

Additional Suggestions

Additional ways to try to identify permitted traffic without legitimate justification and/or high risk

- Weight the results based on traffic which “ages out” without an established session, which would indicate the target system is not listening on the port
- Focus on traffic to/from business critical network zones, such as the industrial control systems or PCI domains
- Focus on traffic inbound to the network from external sources
- Specifically target rules which are not frequently used on the network

Recap

Key Takeaways

1. Your existing Splunk data has valuable insight into the configurations on your network
   - ACTION: Review your sources and identify where Splunk data can help improve to your security posture

2. Your attack surface requires ongoing effort to reduce insecure configurations
   - ACTION: Develop a plan to regularly review activity in the environment for insecure configurations

3. Splunk Enterprise Security includes use cases to identify prohibited traffic
   - ACTION: Configure your ES lookups and apply to your data to find unexpected traffic patterns

Thank You

Don't forget to rate this session in the .conf18 mobile app

.conf18

splunk>