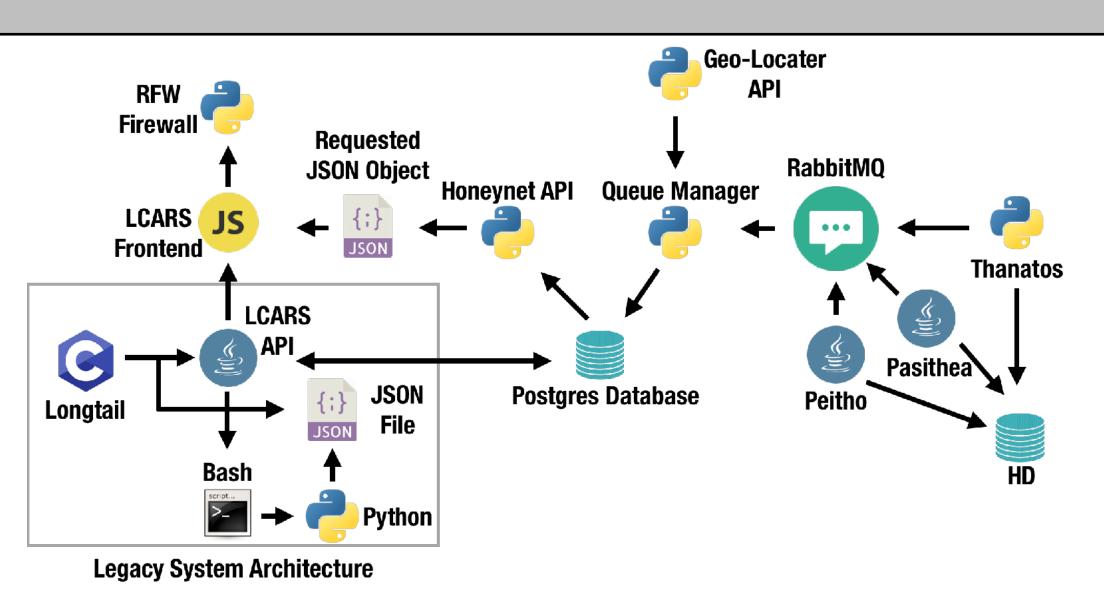
# **LCARS:** Lightweight Cloud Application for Realtime Security

Authors Faculty IBM

Daniel N. Gisolfi and Michael Gutierrez; based on prior work by Graham Burek and Mariah Molenaer Robert Cannnistra, Casimer DeCusatis, Matthew Johnson, Alan G. Labouseur Greg Lacey

#### Overview

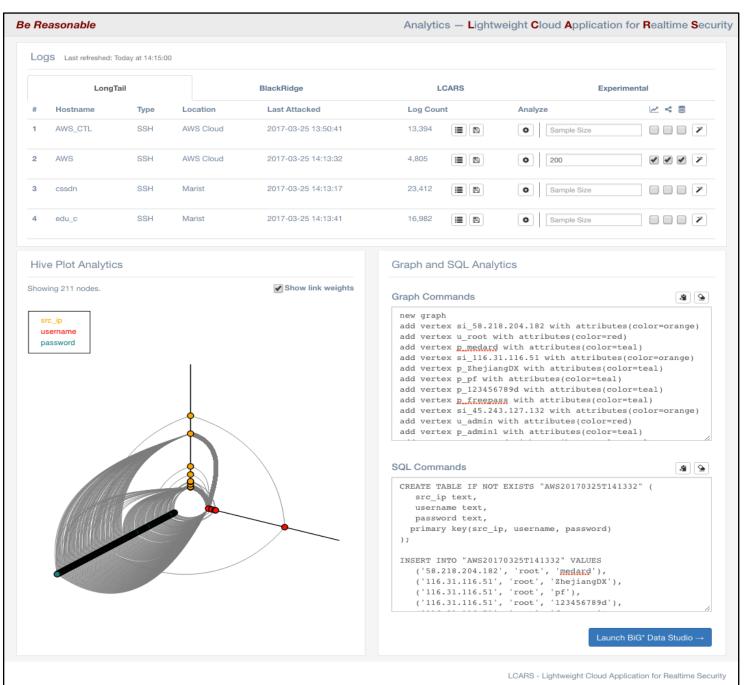


LCARS is a web-based security application designed to identify, analyze, respond to, and help prevent attacks and threats targeting network infrastructure. Using this diagram as a starting point, we divided LCARS into three categories: Analysis, Threat Intelligence, and Threat Response, which we call the Reconfigurator.



This work is sponsored in part by NSF Grant Award 1541384 — CC\*DNI Integration: Application Aware Software-Defined Networks for Secure Cloud Services

### Analysis



We currently take our parsed attack data and generate hive plot visualizations, G\* graph commands, and SQL commands. The graph and SQL commands are sent to BiG\* Data Studio, a front end to the both the G\* graph database and the PostgreSQL. relational database. This allows us to execute our graph and SQL commands and run queries against them. The hive plot pictured on the left represents the same attack data as the graph and SQL on the right.

We are developing automation for process using logs from live routers and SDN controllers so LCARS can dynamically reconfigure the network when it detects an attack.

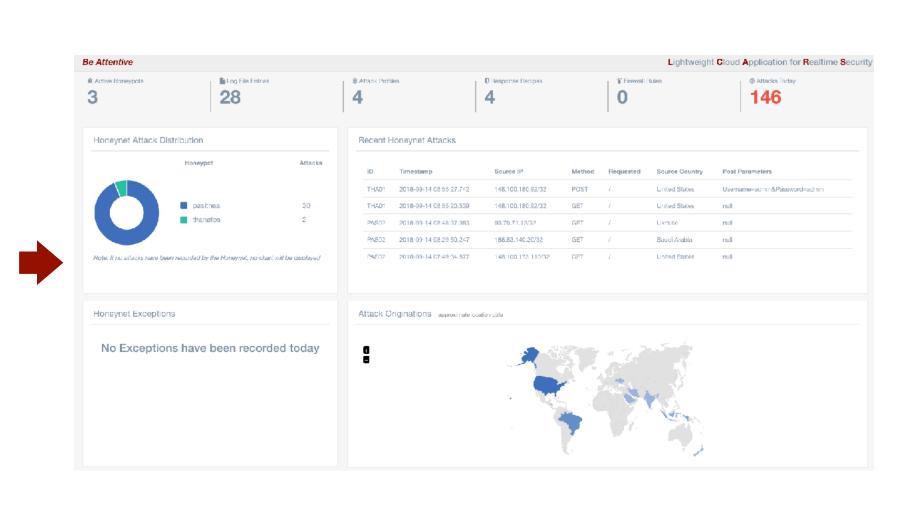
the LCARS Analysis page showing a hive plot, graph commands, and SQL commands generated from attack data

This edition of LCARS builds on prior work by the Marist/IBM Joint Study students and faculty. The honeypot and honeynet components are based on research reported in A HoneyNet Environment for Analyzing Malicious Actors by the same authors. We would like to thank our fellow students as well as the faculty and staff for their support and contributions.

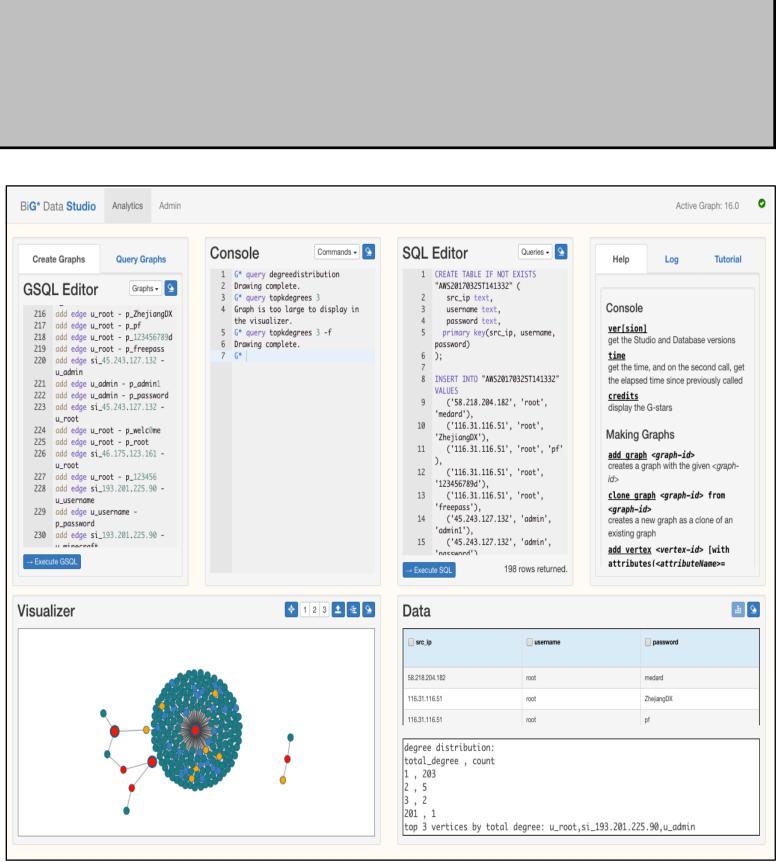
## **Data Collection**

We collect realtime data from our various honeypots within the honeynet using a message queue. Attacks data are cleansed and entered into our database for analysis. This allows for straightforward integration with our relational and graph-based analytics tools. The current infrastructure is scalable and can respond to newly added honeypots on the fly. Additionally we collect live attack data from LongTail SSH honeypots. All attack data is sent as JavaScript Object Notation (JS)

"id": "PAS02",
"timestamp": "2018-09-14 00:00:17.934",
"pot_name": "pasithea",
"host_ip": "10.11.17.23/32",
"host_PID": 1,
"HPID": "null",
"method": "GET",
"requested text": "/",
"source_ip": "187.94.251.93/32",
"source_port": 8080,
"post text": "null",
"source country": "Brazil",
<b>—</b> — — — — — — — — — — — — — — — — — —
},
{
"id": "THA01",
"timestamp": "2018-09-14 00:59:37.604",
"pot_name": "thanatos",
"host ip": "10.11.17.23/32",
"host_PID": 1,
"HPID": "null",
"method": "GET",
"requested text": "/",
"source ip": "177.99.13.19/32",
"source_port": 4400,
"post_text": "null",
"source_country": "Brazil",



Attack data collected from the Honeynet



BiG\* Data Studio showing a graph of the LCARS-generated data running the Top-K Degrees query

SON)	to	the	LCARS	frontend	•

	Tł	٦re	eat	In
Res	ponse De	etails: Figh	t the Power	
#	Target	Chain	Protocol	Source
1	Reject	Input	UDP	4.3.2.1
2	Reject	Input	TCP	1.2.3.4
3	Reject	Input	ICMP	2.3.4.5

The Response Orchestration section of the Threat Intelligence pag

We built a Threat Intelligence database of *attack profiles, response* recipes, and orchestrated responses. A response recipe is a collection of firewall rules. An orchestrated response maps an attack profile to a group of response recipes. To interact with this database we built our own REST API. Our API enables us to easily create, update, and delete database items directly from our GUI.



The Reconfigurator enables deployment of response recipes and orchestrated responses to our firewall. We utilize RFW (Remote Firewall), an open-source REST API for *iptables*, in order to seamlessly interact with the firewall service. Firewall rules can be deployed both in batch or on an individual basis.

Response Recipe	S	
Name	Actions	
Close the Doors	C	
Turn Out the Lights	C	
Cower in Fear	C	
Fight the Power	C	
Add rule	All TCP UDP	
Whitelist	ICMP	
127.0.0.1		
10.0.0/8		
148.100.0.0/16		

Attack data displayed in LCARS





### ntelligence

Destination 0.0.0.0	<b>/</b>		
0.0.0.0	<b>&gt;</b>	Details for the response recipe: Fight the Power	
0.0.0.0			
Add	New Detail Close		
🤹 Respor	ase Orchestration		
Respor	Close the Doors Fight	ht the Power	
	Close the Doors, Figh	ht the Power	
BlackRidge B	eness Close the Doors, Figh 6 steps Cower in Fear 3 steps Turn Out the Lights		

Ridge BlacklistImage: Comparison of the c	estrated Resp	oonses	Re	econfigu	ator Lo	g			
ide in Lameness       Image: Second Sec	ne	Actions		IMan OF	0017	15,00,44		Torrest D	
Image: Second	ckRidge Blacklist	C		-					
Ide in Sarcasm       C         Ide in Dude-ness       Image: Signature Signate Signate Signature Signature Signature Signature Sign	ile in Lameness	C		-			2		2
Ile in Dude-ness       Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:37:44] Action: Add; Target: Reject; Chara         Image: Mar 25 2017 15:3	le in Sarcasm	C		-			-		
#       Target       Chain       Protocol       Source       Destination       Actions         1       Reject       Input       TCP       2.3.4.5       0.0.0.0/0       Image: Component and the second a	ile in Dude-ness	C					-		
#       Target       Chain       Protocol       Source       Destination       Actions         1       Reject       Input       TCP       2.3.4.5       0.0.0.00       imiteation         2       Drop       Input       ICMP       4.3.2.1       0.0.0.00       imiteation         3       Drop       Input       TCP       1.2.3.4       0.0.0.00       imiteation         4       Reject       Input       UDP       116.31.116.51       0.0.0.00       imiteation         5       Drop       Input       All       58.218.204.182       0.0.0.00       imiteation									
#TargetChainProtocolSourceDestinationActions1RejectInputTCP2.3.4.50.0.0.0/0Imit2DropInputICMP4.3.2.10.00.0/0Imit3DropInputTCP1.2.3.40.00.0/0Imit4RejectInputUDP116.31.116.510.00.0/0Imit5DropInputAll58.218.204.1820.00.0/0Imit									
1       Reject       Input       TCP       2.3.4.5       0.0.0.0/0       im         2       Drop       Input       ICMP       4.3.2.1       0.0.0.0/0       im         3       Drop       Input       TCP       1.2.3.4       0.0.0.0/0       im         4       Reject       Input       UDP       116.31.116.51       0.0.0.0/0       im         5       Drop       Input       All       58.218.204.182       0.0.0.0/0       im			Ei	rewall Sta	ate 📿				
1       Reject       Input       TCP       2.3.4.5       0.0.0.0/0       im         2       Drop       Input       ICMP       4.3.2.1       0.0.0.0/0       im         3       Drop       Input       TCP       1.2.3.4       0.0.0.0/0       im         4       Reject       Input       UDP       116.31.116.51       0.0.0.0/0       im         5       Drop       Input       All       58.218.204.182       0.0.0.0/0       im									
2       Drop       Input       ICMP       4.3.2.1       0.0.0.0/0 <ul> <li>3</li> <li>Drop</li> <li>Input             TCP</li> <li>1.2.3.4</li> <li>0.0.0.0/0</li> <li>4</li> <li>Reject</li> <li>Input</li> <li>UDP</li> <li>116.31.116.51</li> <li>0.0.0.0/0</li> <li>5</li> <li>Drop</li> <li>Input</li> <li>Ali</li> <li>58.218.204.182</li> <li>0.0.0.0/0</li> <li>1</li> </ul>			#	Target	Chain	Protocol	Source	Destination	Actions
3         Drop         Input         TCP         1.2.3.4         0.0.0.0/0         1           4         Reject         Input         UDP         116.31.116.51         0.0.0.0/0         1           5         Drop         Input         All         58.218.204.182         0.0.0.0/0         1			1	Reject	Input	TCP	2.3.4.5	0.0.0/0	
4         Reject         Input         UDP         116.31.116.51         0.0.0.0/0         m           5         Drop         Input         All         58.218.204.182         0.0.0.0/0         m			2	Drop	Input	ICMP	4.3.2.1	0.0.0/0	
5 Drop Input All 58.218.204.182 0.0.0.0/0			3	Drop	Input	TCP	1.2.3.4	0.0.0/0	â
			4	Reject	Input	UDP	116.31.116.51	0.0.0/0	1
1 Accept Output All 0.0.0/0 34.22.5.1			5	Drop	Input	All	58.218.204.182	0.0.0/0	<b>b</b>
			1	Accept	Output	All	0.0.0/0	34.22.5.1	â