uila

Application-Centric Cyber Threat Detection

In the recent past, most enterprise organizations have learnt (and most times the hard way) that preventive security methods is not realistic to block all attacks or threats, making it more practical and critical for security teams to prevent those intrusions or vulnerabilities from becoming a data or financial loss. Also, most attacks no longer operate in the "smash and grab" mode, and instead when once inside the network after bypassing perimeter based security systems, now conduct some sort of internal reconnaissance in “stealth” mode. This provides the attacker the golden opportunity to dig in deeper into the entire deployment and also scan for more assets to control to damage. While all organizations have perimeter security and at times end-point security for critical servers and desktop (with security agents), they lag behind in protecting their mission critical "internals" once the threat is inside and is moving laterally in the east-west direction.

Uila assists enterprise organizations combat advanced cyber threats by providing immediate and comprehensive application-centric insight into lateral movement based threats for the Hybrid Enterprise.

Agentless Cyber Threat Monitoring

Agentless and Scalable Deployment model to identify threat challenges for your mission-critical applications, with built-in classification for over 3200 applications.

Application-centric Lateral Movement Threat Detection

Comprehensive Application-centric visibility into lateral (east-west) movement traffic patterns and automated alerting to cyber threats such as malware, DDos, C & C, port scans, Exploit kits, etc.

Anomalous Application Behavior

Confidently track critical Application workload characteristics in real time to identify anomalous behaviors such as dependency changes between the critical application and infrastructure resources, deletion or addition of new VMs, etc.

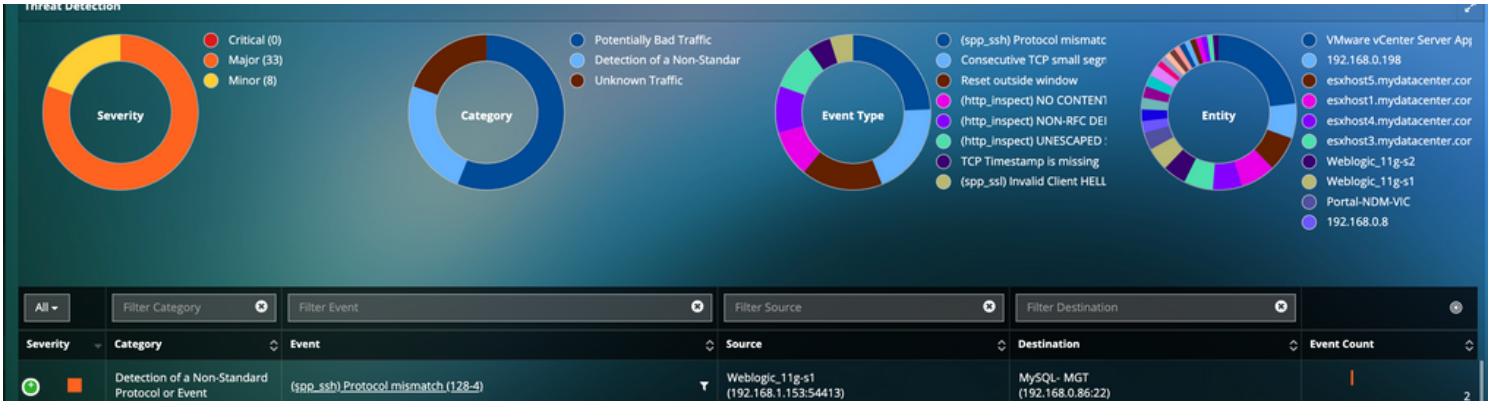
Conclusive Chain of Evidence for any Threat

Identify all application transaction data, infrastructure status and network traffic data before, during and after an attack.

INFO@UILA.COM WWW.UILA.COM +1-408-819-0777

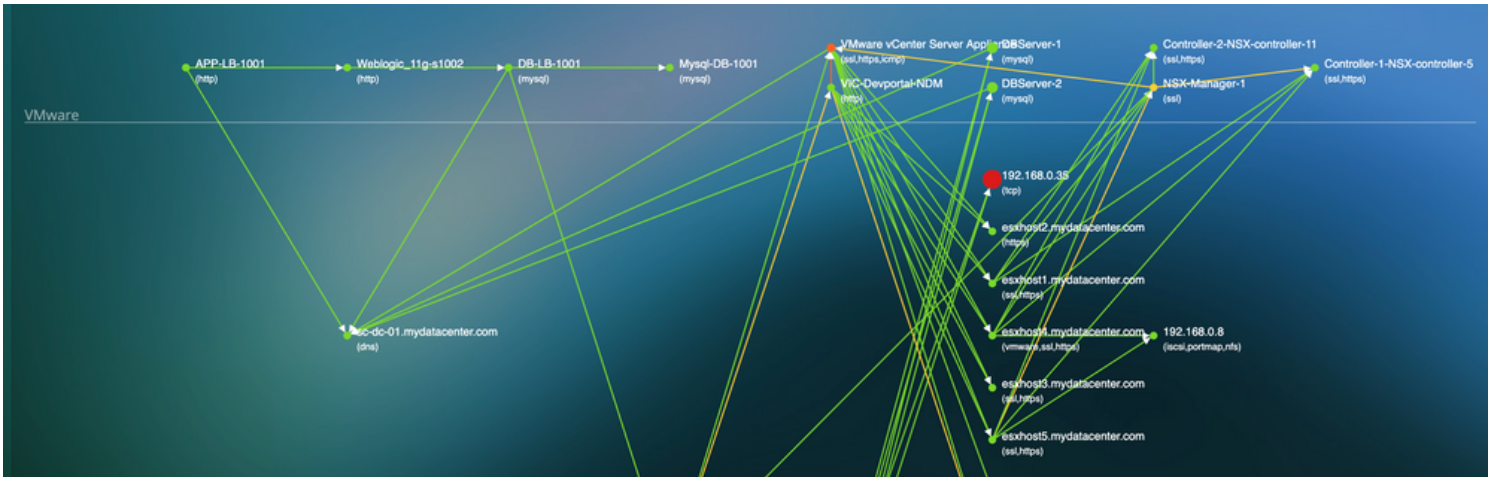
Detect Advanced Malicious Threats in Real-Time for Data Center and Cloud Workloads

- Real-time detection for thousands of emerging threats, including Ransomware, Command & Control, Exploit Kits, Malware Attacks, Port Scans, Obfuscation, SMB Probes, Buffer Overflows, etc.
- Latest signature support and updates from the largest group dedicated to advances in the network security industry .
- Gain overall insights into the historical context of how and the origins of the threats, who is being attacked, time of attack, methods used for the attack, etc.
- Get detailed awareness of Outbound Traffic from your Data Center to the Internet and reduce a huge portion of the risk associated with general Internet connectivity.



Application Anomaly Detection

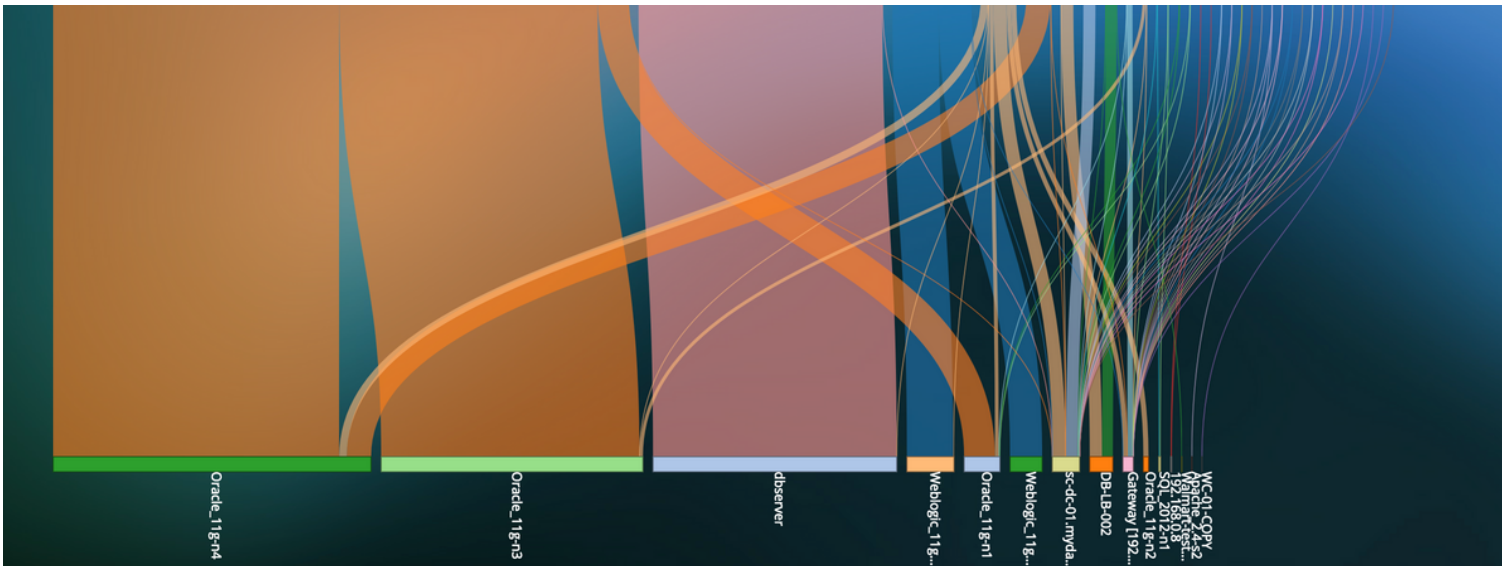
- Automatically classify over 3200 applications and map dependencies across apps & infrastructure.
- Identification of unauthorized VMs and their lateral movement.
- Visualize creation or tearing down of dependencies between assets for a multi-tier application indicating a cyber attack.
- Map thousands of cyber threats directly to the anomalous behavior in application performance and dependencies to identify root-cause.



uila

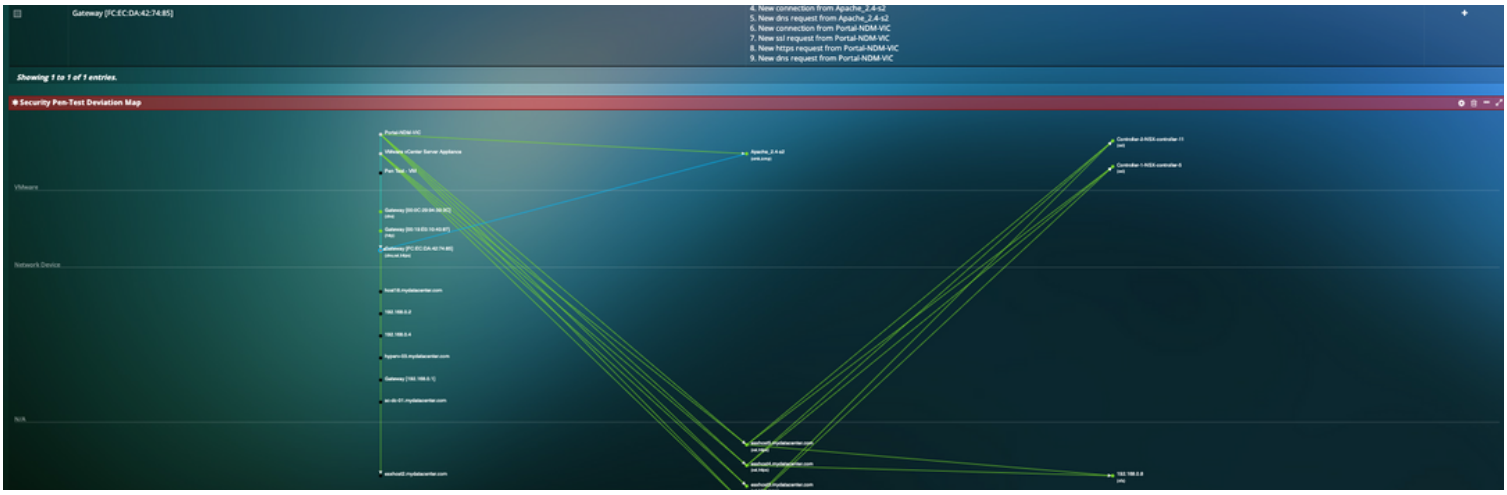
Lateral Movement Traffic Analysis

- Comprehensive visibility into lateral (east-west) movement traffic patterns to identify custom backdoors and compromised systems. For example, including SMB/SMB2 protocols that maybe used to transfer files/malware, password dumpers, etc.
- Identify unauthorized VMs/servers/connections as well as changes in traffic patterns for existing deployments.



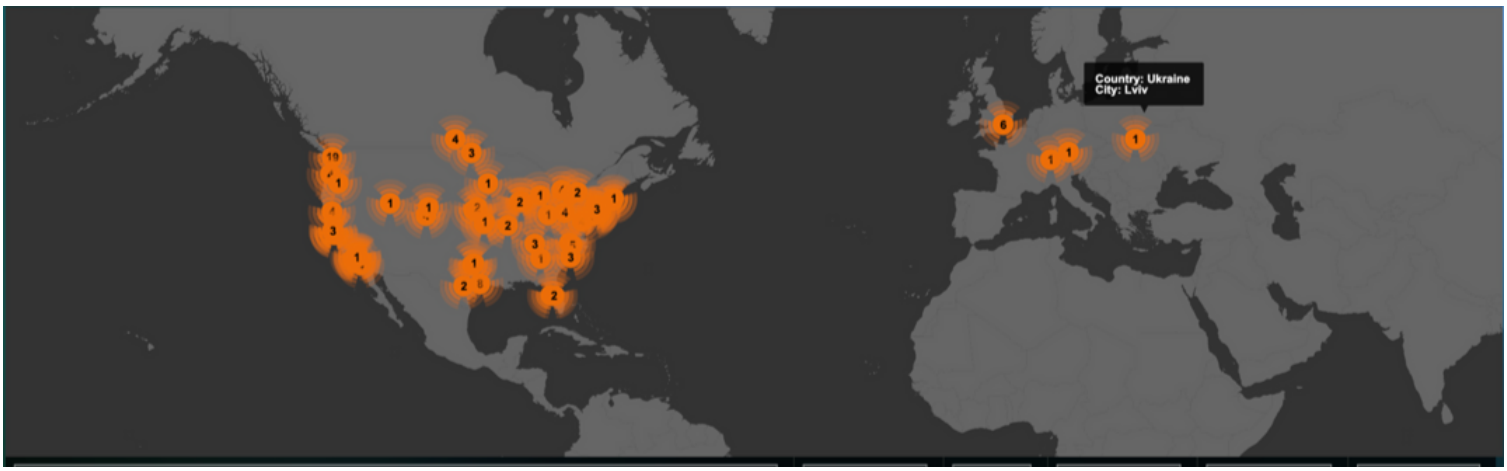
Deep Insights into Current as well as Potential Compromised Assets

- Get detailed information on Dependencies, Process and Infrastructure details (CPU cores, CPU capacity, Memory, Network Traffic) for Compromised systems.
- Know how your currently compromised systems are connected to other mission critical virtual and physical assets as part of the multi-tier application, to get insights into assets that could be compromised next.



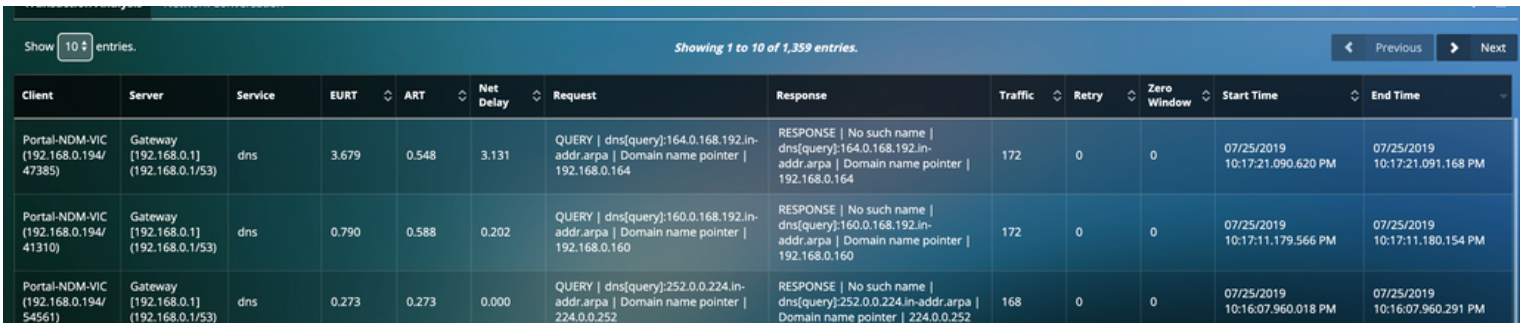
Identify Data Exfiltration activities

- Get detailed awareness of Exfiltration of Traffic from your Data Center to the Internet and reduce a huge portion of the risk associated with general Internet connectivity. Maintain full control over uncontrolled email or file transfers that move proprietary information offsite without proper consent and prevent your network from becoming a participant in a DDoS attack. Some of these outbound transactions may indicate data exfiltration.
- Identify and classify individual attempts of Data Exfiltration to Spam nets identified by Spamhaus (www.spamhaus.org) and Top Attackers listed by DShield (www.dshield.org)
- Visualize Outbound traffic details including Internal VM details, Destination IP, Destination Server location, Application/Service for the outbound traffic, etc.
- Visualize Outbound traffic destinations on a world map.
- Customize and filter Outbound traffic details visualization for your mission-critical service/application group only.



Conclusive Chain of Evidence for any Threat

- Detailed forensic reconstruction to assist security defenders to determine when and how delivery of the cyber threat began.
- Detailed transaction analysis at the application level to analyze time of day for the entire Hybrid environment of when cyber attack began.
- Packet Capture for forensic evidence.



Show 10 entries. Showing 1 to 10 of 1,359 entries. Previous Next

Client	Server	Service	EURT	ART	Net Delay	Request	Response	Traffic	Retry	Zero Window	Start Time	End Time
Portal-NDM-VIC (192.168.0.194/ 47385)	Gateway [192.168.0.1] (192.168.0.1/53)	dns	3.679	0.548	3.131	QUERY | dns[query]:164.0.168.192.in-addr.arpa | Domain name pointer | 192.168.0.164	RESPONSE | No such name | dns[query]:164.0.168.192.in-addr.arpa | Domain name pointer | 192.168.0.164	172	0	0	07/25/2019 10:17:21.090.620 PM	07/25/2019 10:17:21.091.168 PM
Portal-NDM-VIC (192.168.0.194/ 41310)	Gateway [192.168.0.1] (192.168.0.1/53)	dns	0.790	0.588	0.202	QUERY | dns[query]:160.0.168.192.in-addr.arpa | Domain name pointer | 192.168.0.160	RESPONSE | No such name | dns[query]:160.0.168.192.in-addr.arpa | Domain name pointer | 192.168.0.160	172	0	0	07/25/2019 10:17:11.179.566 PM	07/25/2019 10:17:11.180.154 PM
Portal-NDM-VIC (192.168.0.194/ 54561)	Gateway [192.168.0.1] (192.168.0.1/53)	dns	0.273	0.273	0.000	QUERY | dns[query]:252.0.0.224.in-addr.arpa | Domain name pointer | 224.0.0.252	RESPONSE | No such name | dns[query]:252.0.0.224.in-addr.arpa | Domain name pointer | 224.0.0.252	168	0	0	07/25/2019 10:16:07.960.018 PM	07/25/2019 10:16:07.960.291 PM