



Analyzing the CICIDS2017 Dataset: A Comprehensive Incident Response Approach

Presenter Names (Group 27):

Bratt Morejon
Amit Gupta
Alexander Nguyen



Project Overview

- Dataset: CICIDS2017 from the Canadian Institute of Cybersecurity.
- Objective: Analyze the dataset to identify and respond to cybersecurity incidents using professional playbooks and tools.



CICIDS2017 Dataset Overview



- Origin: Created by CIC to address IDS testing gaps.
- Data Type: Network traffic logs, .csv format.
- Technologies Targeted: Ubuntu servers, Windows OS, MAC, and Kali systems.
- Protocols: HTTP, HTTPS, FTP, SSH, Email.



What We Expect to Find?

- DDoS traffic volume may amplify with multiple attackers.
- NAT firewalls should integrate other devices for better security.
- Older OS like Win Vista require constant updates and service management.

CERT Societe Generale Playbook

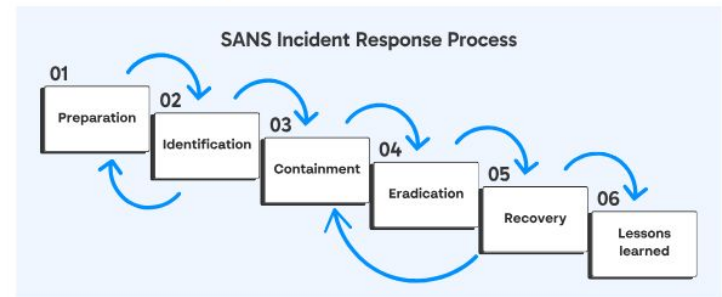
- Developed by CERT Societe Generale.
- Target Audience: SOC analysts, response teams, cybersecurity pros.
- Matches dataset assumptions but requires adaptation for specific attack types.

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

SANS Incident Response Plan





Incident Response Tools

- **Wireshark:** Analyze network traffic.
- **Splunk:** Visualize and correlate data.
- **VirusTotal & AbuseIPDB:** Scan IP addresses.
- **Auditd:** Monitor file changes.



AbuseIPDB



Σ VIRUSTOTAL



Monitoring the Dataset & Asset Identification

Identified unauthorized access and malware attacks :

- Brute Force, XSS, SQL Injection attacks.
- FTP-Patator and SSH-Patator attacks.

205.174.165.73 IP Address Information

ISP	Canadian Institute for Cybersecurity
Usage Type	Fixed Line ISP
Hostname	ip-205-174-165-73.xplore.ca
Domain Name	cyberpsyc.com
Country	 Canada
City	Saint John, New Brunswick

0

/ 62

Community Score

No security vendors flagged this file as malicious

28e9c39256f9d29bd501b0a5dba87d42efe37562b42a9118f39120211b0d0b0d

Thursday-WorkingHours-parts_00034_20170706094058.pcap

cap

Reanalyze Similar More

Size
23.05 MB

Last Analysis Date
a moment ago

CAP

frame matches "UNION"						
No.	Time	Source	Destination	Protocol	Length	Info
4060	2017-07-06 08:11:07.220841	dsg.bttag.com	ubuntu14-64.local	TLSv1.2	1514	Server Hello
4060	2017-07-06 08:11:07.221732	dsg.bttag.com	ubuntu14-64.local	TCP	1514	[TCP Spurious Retransmission] https(443) → 59815 [ACK] Seq=8689 Ack=182 Win=43264 Len=1448 TSval=2990682454 TSecr=36138 [TCP PDU reassembled]
4063	2017-07-06 08:11:07.257061	dsg.bttag.com	ubuntu14-64.local	TCP	1514	[TCP Spurious Retransmission] https(443) → 59815 [ACK] Seq=16385 Ack=182 Win=43264 Len=1448 TSval=2990682482 TSecr=36145
3973	2017-07-06 09:27:48.199876	dsg.bttag.com	ubuntu14-32.local	TLSv1.2	1514	Server Hello
3973	2017-07-06 09:27:48.200759	dsg.bttag.com	ubuntu14-32.local	TCP	2962	[TCP Spurious Retransmission] https(443) → 54810 [ACK] Seq=7241 Ack=182 Win=43264 Len=2896 TSval=2995283436 TSecr=1237640 [TCP PDU reassembled]
3973	2017-07-06 09:27:48.223144	dsg.bttag.com	ubuntu14-32.local	TLSv1.2	1514	[Certificate Fragment]
4066	2017-07-06 09:35:56.213430	b.global-ssl.fastly...	mitacs-pc5.Testbed1...	TCP	1514	http(80) → 60861 [ACK] Seq=1019991 Ack=10416 Win=55808 Len=1460 [TCP PDU reassembled in 4067072]
4140	2017-07-06 09:40:22.025267	172.16.0.1	192.168.10.50	HTTP	603	GET /dv/vulnerabilities/sqli/?id=1%27+and+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1
4150	2017-07-06 09:40:33.465558	172.16.0.1	192.168.10.50	HTTP	666	GET /dv/vulnerabilities/sqli/?id=1%27+and+1%3D1+union+select+null%2C+table_name+from+information_schema.tables%23&Submit=Submit HTTP/1.1
4158	2017-07-06 09:41:07.296717	172.16.0.1	192.168.10.50	HTTP	665	GET /dv/vulnerabilities/sqli/?id=1%27+and+1%3D1+union+select+user%2C+password+from+users%23&Submit=Submit HTTP/1.1
4159	2017-07-06 09:41:20.993268	172.16.0.1	192.168.10.50	HTTP	589	GET /dv/vulnerabilities/sqli/?id=1%27&Submit=Submit HTTP/1.1
4166	2017-07-06 09:41:34.346566	172.16.0.1	192.168.10.50	HTTP	602	GET /dv/vulnerabilities/sqli/?id=1%27+and+1%3D1%23&Submit=Submit HTTP/1.1
4167	2017-07-06 09:41:46.490005	172.16.0.1	192.168.10.50	HTTP	603	GET /dv/vulnerabilities/sqli/?id=1%27+and+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1



Conclusion:

Findings:

- The CICIDS2017 dataset revealed common attack patterns like SQL Injection, Brute Force, and DDoS attacks.
- Tools like Wireshark, Splunk, and VirusTotal were vital for traffic analysis and threat identification.
- The CERT Societe Generale Playbook provided a structured and effective incident response framework.

Key Lessons Learned:

- Realistic datasets improve IDS/IPS training and threat detection.
- Proactive measures like updates and robust firewall rules reduce vulnerabilities.
- Flexible playbooks are crucial for handling diverse attack scenarios.

Impact:

- Enhanced preparedness and actionable insights for minimizing downtime and data loss.
- Improved understanding of effective cybersecurity practices to tackle real-world threats.



Contact info

alexanderhonguyen19@gmail.com

amitgupta44347@gmail.com

bratmorejon@gmail.com

Source:

<https://www.unb.ca/cic/datasets/ids-2017.html>