Data/Hora	Processo	Programa	PID	Usuário	IP Origem	IP Destino	Comando/Eventos	Observações
2025-07-09 02:55:12	cron	crond	4012	root	localhost	localhost	Execução agendada: backup.sh	Rotina de backup
2025-07-09 03:01:45	systemd	systemd	4001	root	localhost	localhost	Inicialização do sistema	Processo padrão
2025-07-09 03:12:20	sshd	sshd	4520	admin	192.168.10.34	10.0.0.12	Accepted password	Login legítimo
2025-07-09 03:18:33	rsyslogd	rsyslogd	4034	root	localhost	localhost	Log rotation	Processo comum
2025-07-09 03:22:05	bash	bash	4555	jose	192.168.10.55	localhost	Executou: cat /etc/passwd	Rotina de consulta
2025-07-09 03:25:10	python3	python3	4587	unknown	203.0.113.45	10.0.0.12	Executou: script brute_force.py	Comando malicioso detectado
2025-07-09 03:26:10	sshd	sshd	4589	unknown	203.0.113.45	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:26:35	sshd	sshd	4591	unknown	203.0.113.45	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:27:01	sshd	sshd	4593	unknown	203.0.113.45	10.0.0.12	Accepted password	Login suspeito
2025-07-09 03:27:40	sudo	sudo	4601	admin	10.0.0.12	localhost	Executou: /bin/netstat -tulnp	Diagnóstico rede
2025-07-09 03:28:15	bash	bash	4605	admin	10.0.0.12	localhost	Executou: /usr/bin/htop	Monitoramento ativo
2025-07-09 03:29:02	bash	bash	4606	admin	10.0.0.12	localhost	Executou: /usr/bin/nmap -sS 192.168.10.0/24	Scan na rede local
2025-07-09 03:29:50	python3	python3	4610	unknown	203.0.113.45	10.0.0.12	Executou: script sql_injection.py	Ataque detectado
2025-07-09 03:31:22	sshd	sshd	4615	unknown	203.0.113.45	10.0.0.12	Connection closed by user	Conexão suspeita encerrada
2025-07-09 03:33:00	nginx	nginx	4630	www-data	10.0.0.12	localhost	Servindo página inicial	Atividade normal
2025-07-09 03:34:15	mysql	mysqld	4640	mysql	localhost	localhost	Executou query SELECT	Consulta banco de dados
2025-07-09 03:36:10	cron	crond	4650	root	localhost	localhost	Execução agendada: limpeza_logs.sh	Rotina manutenção
2025-07-09 03:37:20	ssh-agent	ssh-agent	4655	jose	localhost	localhost	Gerenciamento de chaves SSH	Processo comum
2025-07-09 03:40:45	python3	python3	4660	unknown	203.0.113.45	10.0.0.12	Executou: script reverse_shell.py	Acesso remoto suspeito
2025-07-09 03:42:30	bash	bash	4665	jose	192.168.10.55	localhost	Executou: rm -rf /tmp/tempfiles	Limpeza arquivos temporários
2025-07-09 03:44:05	sshd	sshd	4670	admin	192.168.10.34	10.0.0.12	Accepted password	Login legítimo
2025-07-09 03:46:50	python3	python3	4680	unknown	203.0.113.45	10.0.0.12	Executou: script data_exfiltration.py	Ataque e exfiltração
2025-07-09 03:48:10	systemd	systemd	4690	root	localhost	localhost	Rotina manutenção	Processo padrão
2025-07-09 03:50:00	ssh	ssh	4700	guest	192.168.10.75	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:50:35	ssh	ssh	4700	guest	192.168.10.75	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:51:03	ssh	ssh	4700	guest	192.168.10.75	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:51:47	ssh	ssh	4700	guest	192.168.10.75	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:52:15	sshd	sshd	4705	guest	192.168.10.75	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:54:30	sshd	sshd	4710	guest	192.168.10.75	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 03:55:55	sshd	sshd	4715	guest	192.168.10.75	10.0.0.12	Accepted password	Login suspeito possível força bruta
2025-07-09 03:57:10	bash	bash	4720	guest	192.168.10.75	localhost	Executou: /usr/bin/whoami	Comando básico
2025-07-09 03:59:05	python3	python3	4730	unknown	198.51.100.22	10.0.0.12	Executou: script reconnaissance.py	Scan e reconhecimento
2025-07-09 04:01:40	sshd	sshd	4740	unknown	198.51.100.22	10.0.0.12	Failed password	Tentativa inválida
2025-07-09 04:03:25	sshd	sshd	4750	unknown	198.51.100.22	10.0.0.12	Accepted password	Login suspeito