Arbitr Security

ThreatOps Platform

Arbitr was founded to simplify incident response and threat-hunting processes. We are bringing a new way to automate the complex process of responding, remediating, and reporting cyber incidents.

Overview

The Arbitr ThreatOps Platform, based on our GIBSEN Threat Matrix timeline, is the industry's first platform to automate incident inventions and governance reporting.

- API automation of incident and threat investigations
- Automated incident timeline generation
- Team collaboration and ticketing systems APIs
- Develop TTPs to prevent future attacks
- Automated and consolidated governance reporting
- Create cyber training tools to create institutional knowledge

Key Benefits

45% savings on the cost to investigate, respond, resolve, and report on cyber incidents

50% faster remediation and risk reduction for cyber incidents

60% efficiency improvement during your threat analysis resources and security tools

The Security Investigation Challenge

Today, enterprises and government agencies spend millions building security technology stacks, integration services, and cyber threat intelligence to improve their cyber security posture. Your analyst and threat-hunting teams are left to assess threats, conduct investigations, and produce governance reporting, which are still predominantly manual processes.

This requires the most constrained and expensive resources of your security analyst and threat-hunting teams, which will be occupied for three to four weeks doing the necessary homework to produce incident reports. Based on survey data, over 1000 cyber professionals producing these reports can occupy 100-150 staff hours over 30-45 days to create required reporting for the CSIO, executives, BoDs, auditors, and cyber insurance providers.

To address this challenge, Arbitr has developed a new methodology to use APIs and our new GIBSEN (Graphical Information Base for Security Event Notifications) investigation diagrams, which automate these manual processes that consume the most expensive and scarce cyber resources and provide full reporting for multiple audiences, map the incident to numerous cyber frameworks (MITRE ATT&CK, NIST, Mandinat, etc.). We can scale your cyber resources, accelerate incident reporting, and improve the time to deliver cyber reports from weeks to days.

The Arbitr ThreatOps Platform

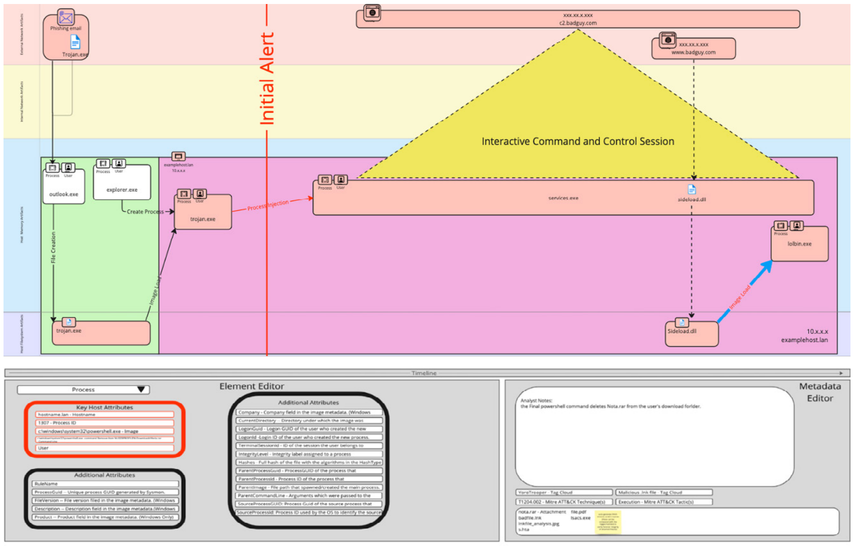
The Arbitr ThreatOps Platform is a new API-driven solution that automates incident investigations for security alerts and threat hunting. The platform is API-driven to source incident information from the leading security tools and cyber threat intelligence reports. Our platform enables your security teams to rapidly assess, investigate, and report cyber incidents efficiently, data-driven, and collaboratively.

API Incident Management

Arbitr acts as your incident management "console" that can source cyber alerts and cyber threat intelligence feeds to create incident timelines, remediation plans, cyber TTP improvement rules, and governance reporting. Arbitr reduces the time and cost of addressing cyber incidents and threat hunting. Our GIBSEN incident timelines:

1. Start with the first alert and place that on the GIBESN incident timeline.
2. Next, you can run queries or assign tickets to your team to move backward in time to the source, and each step populates the GIBSEN timeline.
3. Next, you can move forward in time to map the impact/actions taken as part of this incident to create a complete end-to-end timeline with associated technical details.
4. A remediation plan can be developed, and tickets assigned to eradicate all artifacts from the incident.
5. Create new TTPs to prevent similar attacks in the same category.
6. Report incidents for governance purposes for boards, auditors, regulators, and cyber insurance providers.

Arbitr ThreatMatrix



Key Host Attributes
- hostname.lan - Hostname
- 1307 - Process ID
- c:\windows\system32\powershell.exe - Image
- User

Additional Attributes
- RuleName
- ProcessGuid -- Unique process GUID generated by Sysmon.
- FileVersion -- File version filed in the image metadata. (Windows
- Description -- Description field in the image metadata.(Windows
- Product -- Product field in the image metadata. (Windows Only)

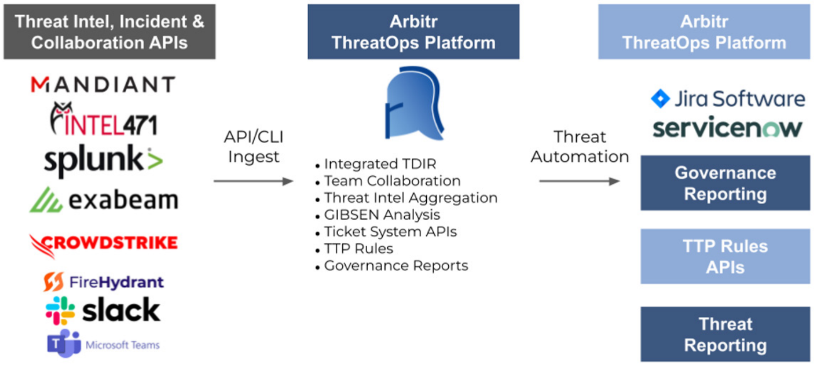
Additional Attributes
- Company - Company field in the image metadata. (Windows
- CurrentDirectory -- Directory under which the image was
- LogonGuid - Logon GUID of the user who created the new
- LogonId -Login ID of the user who created the new process.
- TerminalSessionId - ID of the session the user belongs to
- IntegrityLevel - Integrity label assigned to a process
- Hashes - Full hash of the file with the algorithms in the HashType
- ParentProcessGuid - ProcessGUID of the process that
- ParentProcessId - Process ID of the process that
- ParentImage - File path that spawned/created the main process.
- ParentCommandLine - Arguments which were passed to the
- SourceProcessGUID: Process Guid of the source process that
- SourceProcessId: Process ID used by the OS to identify the source

Analyst Notes:
the Final powershell command deletes Nota.rar from the user's download forlder.

- YoroTrooper - Tag Cloud
- Malicious .lnk file - Tag Cloud
- T1204.002 - Mitre ATT&CK Technique(s)
- Execution - Mitre ATT&CK Tactic(s)

nota.rar - Attachment
badfile.lnk
lnkfile_analysis.jpg
s.hta
file.pdf
lsacs.exe

Automation, Acceleration, & Visualization



Threat Intel, Incident & Collaboration APIs

API/CLI Ingest

Arbitr ThreatOps Platform

- Integrated TDIR
- Team Collaboration
- Threat Intel Aggregation
- GIBSEN Analysis
- Ticket System APIs
- TTP Rules
- Governance Reports

Threat Automation

Arbitr ThreatOps Platform

Governance Reporting

TTP Rules APIs

Threat Reporting

Business Impact

The Arbitr ThreatOps Platform accelerates your time to respond, remediate and report on cyber incidents. It will make your team more effective, improve your security posture with TTPs and demonstrate to leadership, auditors, regulators, and cyber insurance providers that your security team is proactively driving continuous security improvements to prevent future attacks.

www.arbitrsecurity.com