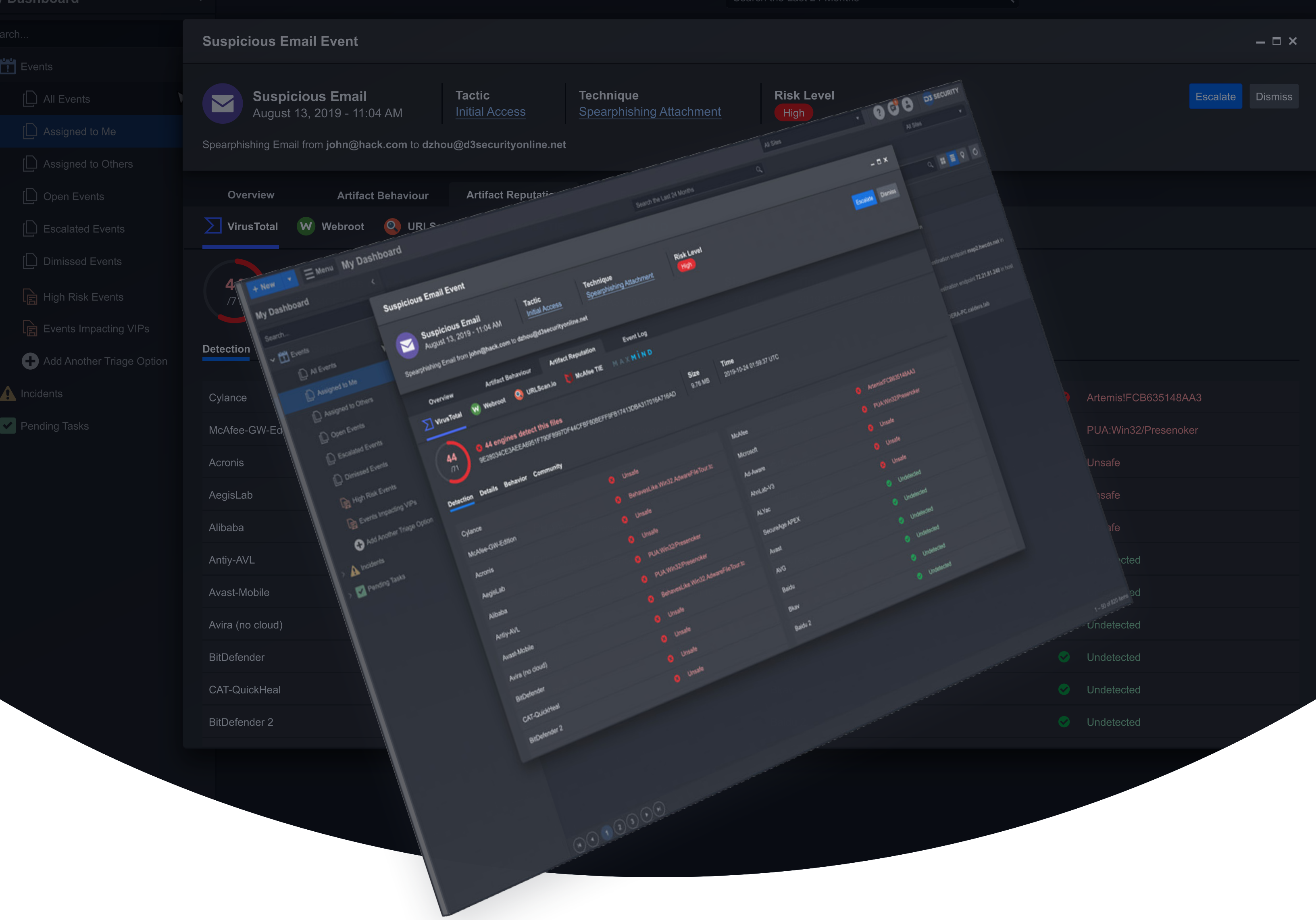
D3 SECURITY ☎ 1-800-608-0081 www.d3security.com sales@d3security.com

TTP-BASED THREAT HUNTING

WITH D3 XGEN SOAR AND MITRE ATT&CK

Security leaders are increasingly looking to the MITRE ATT&CK matrix to help understand and combat the threats against their environment. Security teams who follow ATT&CK can track the tactics being used by adversaries, the scope of attacks, and the efficacy of their controls—generating critical, continuous insights for security operations.

For each technique, MITRE lists detections that security teams can use to identify the presence of the technique in their security data. As detection tools like EDR have become increasingly sophisticated, they are more likely to be able to tag alerts with ATT&CK TTPs. D3 is not a detection tool, so it relies on tools like EDR to make the initial diagnosis of an ATT&CK TTP in an ingested event. However, once the TTP has been tagged, D3 can provide critical functions by sitting on top of the suite of detection tools to enrich events, validate TTP correlations, eliminate false positives, and hunt for more traces of the attack.



Suspicious Email Event

Suspicious Email
August 13, 2019 - 11:04 AM

Tactic: Initial Access

Technique: Spearphishing Attachment

Risk Level: High

Spearphishing Email from john@hack.com to dzhou@d3securityonline.net

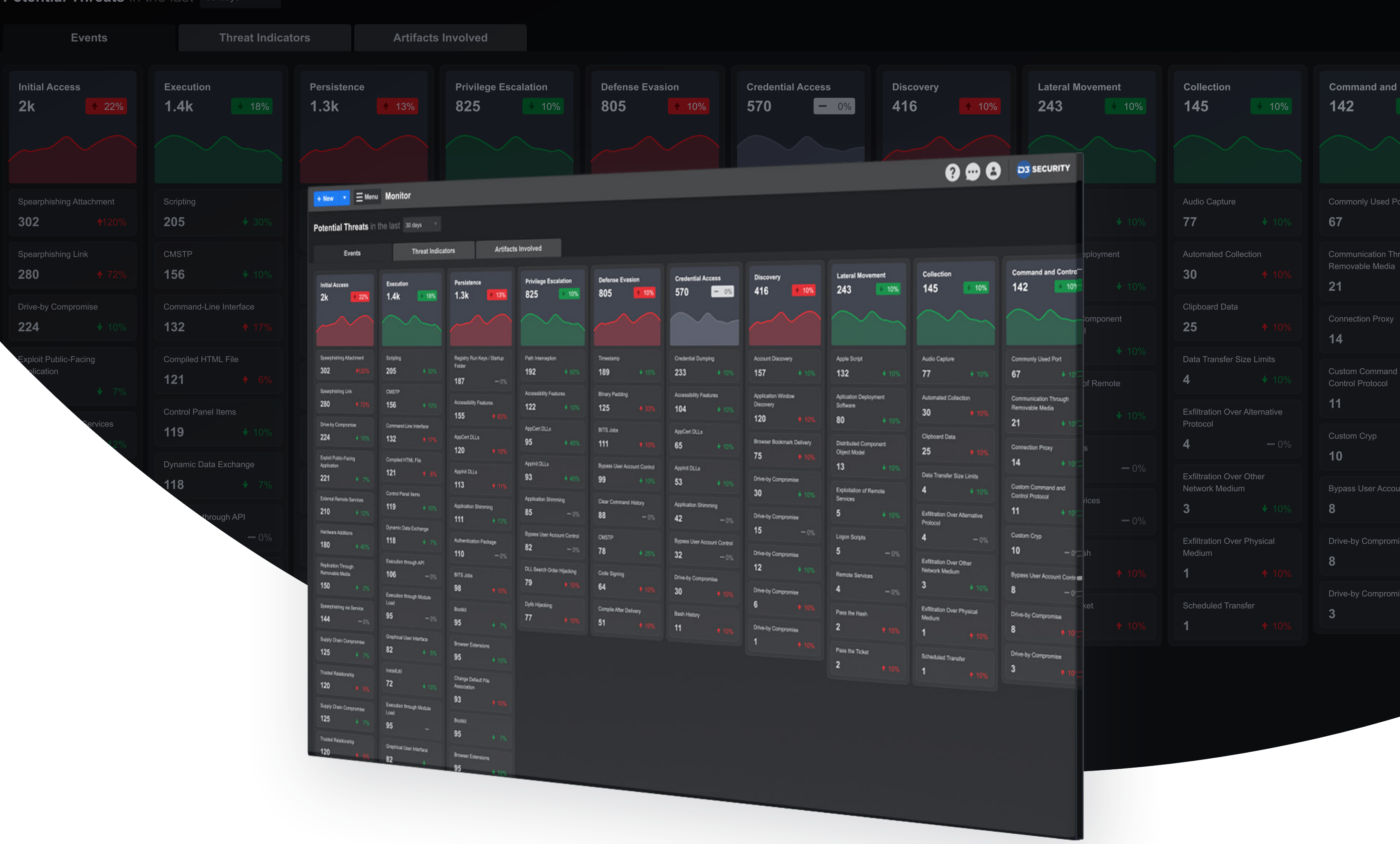
Cylance	Artemis!FCB635148AA3
McAfee-GW-Ed	PUA:Win32/Presenoker
Acronis	Unsafe
AegisLab	nsafe
Alibaba	afe
Antiy-AVL	cted
Avast-Mobile	ed
Avira (no cloud)	Undetected
BitDefender	Undetected
CAT-QuickHeal	Undetected
BitDefender 2	Undetected

CORRELATION AND VALIDATION

ATT&CK technique detection isn't just about endpoints. Valuable data is held in network, firewall, and SIEM logs, as well as DLP tools. Many of these tools are beginning to correlate events against ATT&CK criteria and tag the event with any detected techniques. However, this detection isn't a sure thing. For example, NDR tools can have very broad detections that will result in a lot of false positives unless they are cross-referenced.

D3's connectors span across the entire security stack, including EDR, NDR, firewall, SIEM, and DLP. So, D3 can ingest the event from the detection tool, along with the ATT&CK technique information, and automatically trigger a TTP-specific playbook, which includes querying the rest of the tools to confirm the assessment that the ATT&CK technique is present.

MITRE has recommended detections and mitigations for each technique, which can be worked into D3's playbooks, allowing it to correlate and respond to the technique effectively. Playbooks give D3 SOAR an edge over a SIEM for this use-case, because D3 can search SIEM logs as part of a playbook, whereas a SIEM might have the logs from the other tools, but doesn't have playbooks to orchestrate correlation and remediation.



THE MONITOR DASHBOARD

D3's Monitor Dashboard provides a visual representation of the ATT&CK techniques and sub-techniques detected in the events and incidents generated in the environment. The dashboard centralizes all the technique detections and mappings provided by integrated EDR and NDR solutions, which allows the organization to easily understand its security posture and take actions accordingly to fill gaps.

The Monitor module also supports custom detection and mapping rules for each technique based on the event data that is normalized into D3's data model fields, as well as the creation of custom tactics and techniques. For example, an organization could create a custom tactic that used ingested DNS alerts to get visibility into server monitoring.

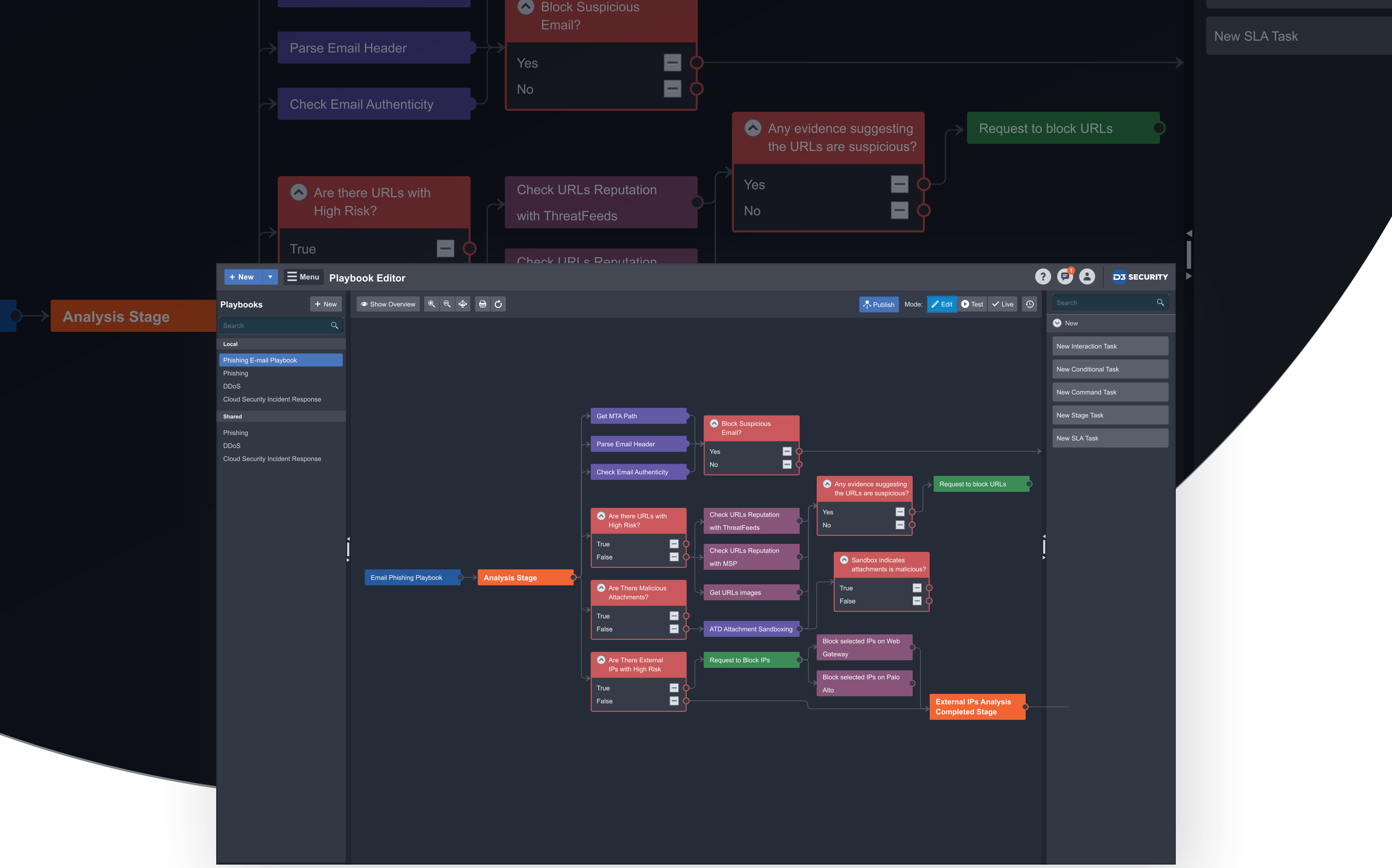
The Monitor Dashboard can be used at various levels of the SOC. For example:

FOR ANALYSTS

A spike in the number of events that involve techniques associated with the Execution tactic could allow the security team to notice malware attacks hitting the organization and turn their focus to triaging the EDR alerts.

FOR SOC MANAGERS

Seeing a large number of events associated with the Impact tactic (the final stage of an attack) could raise alarms and prompt a deeper analysis into their security posture.


Playbook Editor
Playbooks
Local
Phishing E-mail Playbook
Phishing
DDoS
Cloud Security Incident Response
Shared
Phishing
DDoS
Cloud Security Incident Response
Show Overview
Publish
Mode: Edit Test Live
New
New Interaction Task
New Conditional Task
New Command Task
New Stage Task
New SLA Task
Email Phishing Playbook
Analysis Stage
Get MTA Path
Parse Email Header
Check Email Authenticity
Block Suspicious Email?
Yes
No
Any evidence suggesting the URLs are suspicious?
Request to block URLs
Are there URLs with High Risk?
True
False
Check URLs Reputation with ThreatFeeds
Check URLs Reputation with MSP
Get URLs images
Sandbox indicates attachments is malicious?
Are There Malicious Attachments?
ATD Attachment Sandboxing
Are There External IPs with High Risk
Request to Block IPs
Block selected IPs on Web Gateway
Block selected IPs on Palo Alto
External IPs Analysis Completed Stage
D3 SECURITY

TTP CORRELATION AND THREAT HUNTING PLAYBOOKS

D3's low-code playbooks enable TTP correlation and threat hunting. TTPs can be added to events and incidents either automatically, through ingesting events that have been tagged with TTPs by detection tools, or manually.

D3's Tier 3 threat hunting playbooks are designed to contextualize security events through integrations across the environment, connecting Identity, Email, Endpoint and Network tools as data sources. D3 SOAR's robust playbook engine can scale to process complex threat hunting activities that can:

- Identify connections between an event under investigation and another event or artifact that is known to be malicious
- Uncover the parent/child relationship of processes executed and the user accounts responsible
- Widen the scope across the organization and find related IOCs, such as other users that have received the same suspicious email or other hosts that contain the same malicious file hash

USE CASE: CREDENTIAL DUMPING

A D3 playbook monitors incoming incident data for TTP tagging from detection tools. So when ATT&CK technique T1003, Credential Dumping, is identified by an EDR tool and ingested into D3, D3 triggers the Credential Dumping playbook as a nested playbook within the larger use-case-based workflow.

The Credential Dumping playbook then sends notifications to the relevant stakeholders. It also runs a SIEM query to find all other credential dumping events and extract the following data:

- Powershell command line executed
- Name of the host on which the command was executed
- The user who executed the command

Simultaneously, D3 queries Active Directory to enrich the results with computer details, access logs, and more. The identified host information is then further contextualized by running an EDR query to collect more details. The host can be isolated based on the findings and the analyst's confirmation. The playbook can also search the environment for related TTPs, based on the known techniques of threat actors that are suspected to be involved.